የዜጎች የሳይበር ደህንነት ንቃተ-ህሊና ደረጃ በኢትዮጵያ

ኢመደአ /2016

ምስጋና

ይህን ጥናት ለማካሄድና ለማሳካት የተለያዩ አካላት ተሳትፎ ወሳኝ ሚና ነበረው፤ እነዚህም፡- በመጀመሪያ ደረጃ ጥናቱን ለማካሄድ ከመጀመሪያው ጀምሮ ሃሳብ ከማመንጨት በተጨማሪ ሙሉ የጥናት ሂደቱ እስከሚጠናቀቅ ድረስ ልዩ ልዩ ተሳትፎ ላደረጉ ባለሙያዎችና አመራሮች ይሁን፡፡

በሁለተኛ ደረጃ ደግሞ ጥናቱ በሚካሄድበት ወቅት በመረጃ ስብሰባ፤ የዳታ ኢንኮዲንግና ማጥራት ስራዎች ለተሳተፉ ባለሙያዎች በሙሉ እንዲሁም በፈቃደኝነት ላይ የተመሰረተ ምላሾችን ለሰጡን የዚህ ጥናት መረጃ ሰጭዎች በሙሉ ምስጋና ይገባል፡፡

በመጨረሻም የዚህን ጥናት አስፈላጊነት ተረድተው ጥናቱ እንዲሳካ መልካም ድጋፋቸውንና ቅን ትብብራቸውን ላደረጉልን በጥናቱ የመረጃ መሰብሰቢያ መዳረሻዎች በሙሉ ለሚገኙ የመንግስትና የግል ድርጅቶች የስራ ሃላፊዎች ምስጋና እናቀርባለን፡፡

አጠቃሎ (Abstract)

ይህ ጥናት መሰረታዊ በሆነ መንገድ በኢትዮጵያ የሳይበር ተጠቃሚ ዜጎች ያለውን የሳይበር ደህንነት ንቃተ-ህሊና ደረጃ ማወቅን ታሳቢ በማድረግ የተከናወነ ሲሆን፤ የጥናቱ ዝርዝር ዓላማዎች ማለትም የቴክኖሎጅውን ተጠቃሚዎች እውቀት፣ አመለካከት እና አጠቃቀም መለካትን ትኩረት በማድረግ ተካሂዷል፡፡ ጥናቱንም ለማከናዎን በመጀመሪያ በሀገር አቀፍ ደረጃ ያለውን የኢንተርኔት ተጠቃሚ ዜጎች የጥናቱ ፖፕሌሽን አድማስ ወሰን በማድረግ ተካሂዷል፡፡ በዚህ መሰረት የጥናቱ ስልት ኳንቲታቲቭ የአጠናን መንገድን የተከተለ (Quantitative Research Design/Approach) ነበር፤ በተጨማሪም ከዚህ የጥናት ስልትና ዓላማ ጋር አብሮ በተሻለ መንገድ ሊሄድ የሚችለውን የዲስክሪፕቲቭ ጥናት ዓይነት (Descriptive ResearchType) ጥቅም ላይ ውሏል፡፡ በዚህ የጥናት ዲዛይንና መንገድ ተስማሚነት መሰረት ከጥናቱ አጠቃላይ ፖፑሌሽን (Reference Population) ውስጥ ፕሮባቢሊቲ ሳምሊንግን (Probability Sampling) በመተግበር ሰርቬይ (Sample Survey) በዋናነትም የባለብዙ ደረጃ ክላስተር ሳምሊንግ የናሙና መረጣ ቴክኒክን (Multi-Stage Cluster Sampling Technique) ናሙናዎችን በኢትዮጵያ ከተመረጡ አስራ ሰባት (17) ከተሞች ውስጥ ከ16ቱ ከትግራይ ክልል (መቀሌ) ዉጭ መረጃዎች እንዲሰበሰቡ ተደርጓል፡፡ በተጨማሪም የተሰበሰቡ መረጃዎች የመተንተኛ እና የአተረጓጎም መንገዶች በግልጽ የተቀመጡ ሲሆን፤ በዚህ መንገድ የተሰበሰቡ መረጃዎች ወደ ትንተና ከመሄዳቸው በፊት የዳታ ማጥራትና ማደራጀት ስራዎች ከተከናወኑ በኋላ መረጃዎችን ወደ መተንተኛ ሶፍትዌር (SPSS Software) በመጠቀም መረጃዎችን እንዲተነተኑ ተደርጓል፡፡ በጥናቱ የመረጃ አቀራረብና ትንተና ምዕራፍ ደግሞ በጥናቱ የመነሻ ችግር ዝርዝር መግለጫ (Problem Statement) ላይ እንደተገለፀው በሀገራችን በብሄራዊ ደረጃ ሊገለጽ የሚችል የሳይበር ደህንነት ንቃተ-ህሊና ሁኔታን ሊያሳይ የሚችል ቀደምት የጥናት ስራዎች ባለመኖራቸው የሃገራችንን የቴክኖሎጅ ተጠቃሚዎች የሳይበር ደህንነት ንቃተ-ህሊና ደረጃ ማዎቅ በማስፈለጉ ጥናቱ ተካሂዷል፡ ፡ የጥናቱ ውጤትም 35% የእውቀት ደረጃ፣ 47% አመለካከት እና 49.8% የቴክኖሎጅ አጠቃቀም ደረጃ ሲሆን አጠቃላይ ሃገራዊ የተጠቃሚዎች የሳይበር ደህንነት ንቃተ-ህሊና ደረጃ 20% መሆኑን ጥናቱ ያሳያል።

ማውጫ

ምስጋና i

አጠቃሎ (Abstract) ii

አህጽሮተ-ቃላት 1

ምዕራፍ አንድ 2

1.1. የጥናቱ ዳራ 2

1.2. የችግሩ ዝርዝር መግለጫ (Statement of the problem) 3

1.3. የጥናቱ አላማ 4

1.3.1. የጥናቱ ዋና አላማ 4

1.3.2. የጥናቱ ዝርዝር ዓላማዎች 4

1.4. የጥናቱ ፋይዳ 4

1.5. የጥናቱ ወሰን 5

1.6 የጥናቱ ውስንነቶች (Limitations of the study) 5

ምዕራፍ ሁለት 6

2.1 የሳይበር ደህንነት 6

2.2 የሳይበር ደህንነት ስጋቶችና የሣይበር ጥቃት 7

2.2.1 የአደጋ ፅንሰ ሃሳብ 7

2.2.2 የሳይበር ደህንነት ስጋቶች እና የስጋት ምንጮች 10

2.2.2.1 የስጋት ምንጮች 10

2.3 የሳይበር ጥቃት እና የሳይበር ጥቃት ዓይነቶች 10

2.4 የሳይበር ደህንነት ንቃተ-ህሊና ባህል ግንባታ (Maturity) ሞዴል 12

2.4.1 የጥናቱ ጽነሰ-ሃሳባዊ ሞዴል (Conceptual framework) 14

ምዕራፍ ሶስት 15

3.1 የጥናቱ አሰራር (Research methods) 15

3.2 የጥናቱ ዲዛይን (Study design) 15

3.3 የጥናቱ ፖፑሌሽን 16

3.4 የጥናቱ ናሙና ቁጥር (Sample size) 16

3.4.1 የናሙና መረጣ ስትራቴጂ (Sampling strategy) 17
3.5 የመረጃ ምንጭ (Data sources) 18
3.6 የመረጃ መሰብሰቢያ መንገዶች (Data collection tools) 18
3.7 የትንተና አካሄድ 18
3.8 የጥናት ስነ-ምግባር (Ethical Considerations) 19

ምዕራፍ አራት 20

የመረጃ አቀራረብ፣ ትንተና እና ትርጓሜ 20
4.1 የስነ-ህዝብ መረጃዎች (Demographic information) 20
የጥናቱ ተሳታፊዎች ዕድሜ 20
የትምህርት ደረጃ 21
የጥናቱ ተሳታፊዎች ፆታ 21
4.2 የሳይበር ደህንነት እውቀት ትንተና 22
4.2.1 አጠቃላይ አማካኝ የእውቀት ደረጃ ውጤት 28
4.3 የሳይበር ደህንነት አመለካከት (Attitude) ትንተና 29
4.3.1 አጠቃላይ አማካኝ የአመለካከት ምዘና ውጤት 37
4.4 የሳይበር ደህንነት ንቃተ-ህሊና አጠቃቀም/ልምምድ ትንተና (Practice analysis) 38
4.4.1 አጠቃላይ አማካይ የሳይበር ደህንነት አጠቃቀም/ልምምድ ምዘና ውጤት 45
4.5 አጠቃላይ የሳይበር ደህንነት ንቃተ-ህሊና ሁኔታ በኢትዮጵያ (Cyber security awareness) 46
4.6 የጥናቱ ትንተና አጭር ማጠቃለያ 47

ምዕራፍ አምስት 49

ማጠቃለያና ምክረ-ሃሳብ 49
5.1 ማጠቃለያ (Conclusion) 49
5.2 ምክረ-ሃሳብ (Recommendations) 50
ማጣቀሻ ጽሁፎች (References) 52

አህጽሮተ-ቃላት

ኢመደአ- የኢንፎርሜሽን መረብ ደህንነት አስተዳደር
የሳ/ደ/ን- የሳይበር ደህንነት ንቃተ-ህሊና
CSA- Central Statistics Agency (Ethiopia)
GSMA- Global System for Mobile Communications
IBM- International Business Machines Corporation
SANS- SysAdmin, Audit, Network and Security
SPSS- Statistical Package for the Social Sciences

ምዕራፍ አንድ

መግቢያ

1.1. የጥናቱ ዳራ

የሳይበር ጥቃት አሁን ባለንበት ዘመን የዓለማችን ትልቁ ስጋት እየሆነ መምጣቱን በርካታ የጥናት ውጤቶችና በዘርፉ ላይ ትኩረት አድርገው የሚሠሩ የልዩ ልዩ ተቋማት ሪፖርቶች ይጠቁማሉ፡፡ በዓለም ዙሪያ የሚፈጸሙ የሳይበር ጥቃቶችም ከጊዜ ወደጊዜ በዓይነትም ሆነ በመጠን በከፍተኛ ደረጃ እየጨመሩ መምጣታቸውንም እነዚህ መረጃዎች ያመላክታሉ፡፡ ለአብነትም በአውሮፓውያኑ 2018/19 ዓመት ብቻ በዓለም አቀፍ ደረጃ ከፍተኛ መጠን ያለው የሳይበር ጥቃት መፈጸሙን "ኦንላይን ትረስት አሊያንስ"(On-line Trust Alliance-OTA) በሪፖርቱ ገልጿል፡፡ የደረሰው ጥቃት በገንዘብ ቢተመን ከ45 ቢሊዮን ዶላር በላይ የሚገመት መሆኑንና በዚህ የተነሳ ዓለማችን ማግኘት የሚገባትን ይህን ያህል ግዙፍ የገንዘብ መጠን ማጣቷንም ሪፖርቱ ያመላክታል፡፡

የሳይበር ጥቃት፤ ከሳይበር ደህንነት ጋር የተያያዙ አደጋዎች፤ ከሳይበር ወንጀሎች፣ የማንነት ስርቆትና ሌሎች ገንዘብ ነክ በሆኑ ጉዳቶች ተወስኖ የማይቀርና የሃገራትን ብሄራዊ ደህንነት አልፎ ተርፎም የዓለማቀፍ ደህንነትን ስጋት ላይ የሚጥል ነው (ስቴቨን፣ 2012)፡፡ በሌላ በኩል የሳይበሩ ኢንዱስትሪ የዓለማችን የፖለቲካና የኢኮኖሚ ማዕከል እየሆነ ከመጣ ውሎ አድሯል፡፡ ሃገራት በኢንደስትሪው አማካኝነት በሚመነጨው ከፍተኛ ገቢ የተነሳ መጠነ ሰፊ ፉክክር ውስጥ መግባታቸውና ይህም ቅድሚያ እንደሚሰጣቸው ሀገራዊ ደህንነትን የሚመለከቱ ፖለቲካዊና ወታደራዊ ጉዳዮች ሁሉ ዘርፉ ቀዳሚ የውድድር መድረክ እየሆነ ስለመምጣቱም በርካታ ማሳያዎች ናቸው፡፡ የ2016ቱ የአሜሪካ ምርጫና ምርጫውን ተከትለው የተከሰቱና በዚያች ሃገር ፖለቲካና ዓለም አቀፋዊ ጉዳዮች ሳይቀር ከፍተኛ ተፅዕኖን መፍጠር የቻሉና እስካሁንም ድረስ መነጋገሪያ የሆኑ ሳይበራዊ ጉዳዮች ለዚህ እንደ ጥሩ ማሳያ ተደርገው ይወሰዳሉ፡፡

ሴሪሊ (2018) የአፍሪካ የሳይበር ደህንነት ሪፖርትን ዋቢ በማድረግ ባጠናዉ ጥናት መሰረት ባለፉት አመታት የሳይበር ጥቃት ባልተጠበቀ ፍጥነት በአለም ላይ በከፍተኛ ቁጥር ጨምሯል፡፡ አፍሪካም እንደ አህጉር ከፍተኛ የሳይበር ጥቃት ገጥሟታል፡፡ ይህም ጉዳት በኢኮኖሚና በማህበረሰብ እድገት ላይ ከፍተኛ ጉዳት አድርሷል፡፡ ለዚህም እንደ ምክንያት የተቀመጡት የሳይበር ደህንነት ንቃተ-ህሊና ዝቅተኛ መሆንና እያደገ የመጣዉ የዲጅታል መሰረተ-ልማቶች እድገት ይጠቀሳሉ፡፡

በሀገራችን ኢትዮጵያም እንደዚሁ የሳይበር ጥቃት በከፍተኛ ደረጃ እየጨመረ መጥቷል፡፡ በዚህም በ2011 ዓ.ም በሃገሪቱ ላይ የደረሱት አጠቃላይ የሳይበር ጥቃቶች 791 የነበሩ ሲሆን በአንድ ዓመት ጊዜ ውስጥ

ጥቃቱ በ296 ጨምሮ በ2012 ዓ.ም የደረሰው አጠቃላይ የሳይበር ጥቃት 1087 መድረሱን የኢንፎርሜሽን መረብ ደህንነት አስተዳደር(ኢመደአ) ሪፖርት ያመላክታል፡፡ የሳይበር ጥቃት አኃዙ በቀጣዮች ዓመታትም በከፍተኛ ደረጃ ጨምሮ በ2013 ዓ.ም 2898 እና በ2014 ዓ.ም 8845 ደርሷል[1] ፡፡

ከነዚህም ጥቃቶች ውስጥ በ2014 ዓ.ም የተቃጡ ጥቃቶችን ብቻ ብንመለከት በመሰረተ ልማት ላይ የሚደርሰዉ ጥቃት የመጀመሪያ ደረጃን ሲይዝ የጥቃቱ መጠንም ወደ 3954 ወይም 44.7 በመቶ አካባቢ ይደርሳል፡፡ የዌብሳይት ጥቃት በበኩሉ ሁለተኛ ደረጃን በመያዝ ከዓመቱ አጠቃላይ የጥቃት መጠን 1800 ማለትም 20 በመቶ አካባቢ የሚሆነውን ድርሻ ይሸፍናል፡፡

ለእነዚህ የሳይበር ጥቃቶች መጨመር እንደምክንያት ከሚቀመጡት መካከል የኢንተርኔት አገልግሎት ተጠቃሚዎች ቁጥር ከጊዜ ወደ ጊዜ እየጨመረ መሄድ የሚጠቀስ ሲሆን በሃገራችን በ2018/19 41.9 ሚሊየን የሞባይል ስልክ ተጠቃሚና 22.3 ሚሊየን ኢንተርኔት ተጠቃሚ [2] እንደነበር ያሳያል፤ ይህም ከ2017/18 ዓመት ጋር ሲወዳደር 15 በመቶ እንዳደገ ያመላክታል (ኢትዮ ቴሌኮም 2018/19)፡፡

በሌላ በኩል የሰዎች የሳይበር ደህንነት ግንዛቤ ማነስ የሳይበር ጥቃት ለሚፈጽሙ ሃከሮችና አጥቂዎች የማህበራዊ ምህንድስናን እና ሌሎችንም ስልቶች በመጠቀም ጥቃት ለመፈጸም እንዲጠቀሙበት አስችሏል፡፡ ከዚህም አኳያ የሰው ልጆች ግንዛቤ ክፍተት ለሚደርሱት 95% የሳይበር ጥቃቶች እንደ ምክንያት ሆኗል (IBM 2015)፡፡

ወረታ እና ለሳ (2012) ባጠኑት ጥናት መሠረት በኢትዮጵያ ውስጥ የሚገኙ ባንኮች ዝቅተኛ የሆነ የኢንፎርሜሽን ደህንነት ንቃተ ሕሊና እንዳላቸው ይገልፃሉ፡፡ በመሆኑም ከጊዜ ወደጊዜ እየጨመረ የመጣዉን የሳይበር ጥቃት ለመከላከልና ለመቀነስ የኅብረተሰቡን የሳይበር ደህንነት ንቃተ ሕሊና ማሳደግ እንደሚያሥፈልግ ጥናቱ ያመላክታል፡፡ ስለሆነም የኅብረተሰቡን የሳይበር ደህንነት ንቃተ ሕሊና በመለካትና ክፍተቶችን በጥናት በተደገፉ ውጤቶች በማሳየት በቀጣይ በኅብረተሰቡ ዘንድ ያለውን የንቃተ ሕሊና ክፍተት መሙላት አስፈላጊ በመሆኑ ኢመደአ ይህንን ጥናት እንዲያካሂድ መነሻ ምክንያት ሆኗል፡፡

1.2. የችግሩ ዝርዝር መግለጫ (Statement of the problem)

እንደ አቤሴሎም ንጉሴ (2015) ጥናት ከሆነ በሃገራችን የባንኪንግ ዘርፍ ከከፍተኛ ሀላፊዎች ጀምሮ ዝቅተኛ የሆነ የሳይበር ደህንነት ንቃተ ህሊና፤ አነስተኛ የኢንዱስትሪ ተሞክሮና የሳይበር ደህንነት ስታንዳርድ ትግበራ በተጨማሪም የሳይበሩ እዉቀት ያላቸዉ የባለሙያዎች እጥረት አሁን ባለዉ የኢትዮጵያ የግልና የመንግስት ባንክ ዘርፍ ችግር ናቸዉ ይላል፡፡

በጂኤስኤምኤ (GSMA) ኢንተለጀንስ አመታዊ ሪፖርት (2019) መሰረት በኢትዮጵያ በ2015/16 ከነበረው 12 ሚሊየን አካባቢ የኢንተርኔት ተጠቃሚዎች ቁጥር ወደ 18 ሚሊየን ያደገ ሲሆን ይህም ከአጠቃላይ ህዝቡ 16% ነዉ፡፡ ከነዚህም ዉስጥ ንቁ የማህበራዊ ሚዲያ ተጠቃሚዉ ከ3.3 ሚሊዮን ወደ 6.1 ሚሊዩን ያደገ ሲሆን ይህም ከአጠቃላይ ህዝቡም 5.6% ገደማ ይሆናል፡፡ በተጨማሪም ከአጠቃላይ ኢንተርኔት ተጠቃሚው ዉስጥ በሞባይል ስልክ የሚጠቀመዉ ህዝብ ላፕቶፕና ዴስክቶፕ ከሚጠቀመዉ ይበልጣል፡፡

1 ይህ አሃዝ የሚያመለክተዉ በኢመደአዉ ኢትዮሰርት የጥቃት ምላሽ ግብረ-ሃይል በየአመቱ ሪፖርት ተደርገዉ ምላሽ የተሰጠባቸዉ ጥቃቶች ብዛት እንጂ አጠቃላይ በሃገር ደረጃ እየደረሰ ያለን የሳይበር ጥቃት አይወክልም፡፡ ከዝቅተኛ የሳይበር ደህንነት ንቃተ-ህሊና ረገድ አብዛኞቹ ጥቃቶች ሪፖርት ሳይደረግባቸዉ ወይም ሳይታወቁ እንደሚቀሩ ይታሰባል፡፡

2 ዳታ ሪፖርታል፡ ድጂታል ኢትዮጵያ 2022 ሪፖርት መሰረት 29.83 ሚሊዮን ኢንተርኔት ተጠቃሚ እንደነበር ያመላክታል

ሪፖርቱ እንደሚያመለክተው የሕብረተሰቡ የኢንተርኔት ተጠቃሚነት ቁጥር በከፍተኛ ደረጃ እየጨመረ የመጣ ሲሆን የሳይበር ጥቃቱም በዛው ልክ እየጨመረ መምጣቱን መገንዘብ ይቻላል፡፡ ስለሆነም የሕብረተሰቡን የሳይበር ደህንነት ንቃት ሕሊና ደረጃ ለማሳደግ አሁን ያለበትን የሳይበር ደህንነት ንቃት ሕሊና ደረጃ ማወቅ ግድ ይላል፡፡ በዚህ ረገድ ኢመደአ[3] በሳይበር ደህንነት ንቃት ሕሊና ግንባታ ዙሪያ የቴሌቪዥንና የሬድዮ ፕሮግራሞችን እንዲሁም በተቋማት ደረጃ የሳይበር ደህንነት የዳሰሳ ጥናቶችን በማድረግ የሕብረተሰቡን እንዲሁም የተቋማትን የሳይበር ደህንነት ግንዛቤ ለማሳደግ እየሠራ ይገኛል፡፡ ይህም ሆኖ አሁን ላይ በሀገር አቀፍ ደረጃ እየደረሰ ካለው የሳይበር ጥቃት አኳያ ይህ ብቻ በቂ ባለመሆኑ፤ ክፍተቶችን በመሙላት የሚደርሰውን ጥቃትና በሃገር ላይ ሊደርስ የሚችለውን ሁለንተናዊ ጉዳት ለመቀነስ በቅድሚያ አጠቃላይ የኢንተርኔት ተጠቃሚ ዜጎችን የሳይበር ደህንነት ንቃት ሕሊና ማወቅ ይገባል፡፡

ይሁን እንጅ በአሁኑ ጊዜ በኢትዮጵያ የዜጎችን የሳይበር ደህንነት ንቃተ ህሊና ማለትም የእዉቀት፣ የአመለካከት፣ እንዲሁም የአተገባበር ደረጃን (Knowledge, Attitude and Practice- KAP) የሚገልጽ የተጠና ጥናት በኢመድአም ሆነ በሌሎች ተቋማት የለም፡፡ በዚህ ምክንያት ወደፊት ምን መደረግ አለበት የሚልና ሌሎች ከሳይበር ደህንነት ጋር የሚነሱ ጥያቄዎችን ለመመለስና ውሳኔዎችን ለማስተላለፍ አዳጋች ያደርገዋል፡፡ በመሆኑም በሳይበር ደህንነት ንቃተ ህሊና ዙሪያ ያለዉን ክፍተት በማወቅ ክፍተቶችን ለመሙላት ይህ የዜጎች የሳይበር ደህንነት ንቃተ ህሊና ጥናት አስፈልጓል፡፡ ስለሆነም ይህ ጥናት በአጠቃላይ ዜጎች ያሉበትን የሳይበር ደህንነት ንቃተ ህሊና ደረጃ ለማወቅ የሚያስችል በዘርፉ የመጀመሪያ ደረጃ ሀገር አቀፍ ጥናት እንደሆነ መረዳት ይቻላል፡፡

1.3. የጥናቱ አላማ

1.3.1. የጥናቱ ዋና አላማ

የዚህ ጥናት ዋና ዓላማ በኢትዮጵያ የሳይበር ተጠቃሚ የሆኑ ዜጎችን የሳይበር ደህንነት ንቃት ሕሊና ደረጃ በማወቅ በቀጣይ የንቃተ ሕሊና ክፍተትን ለመሙላት የሚያስችሉ ፕሮግራሞችን ለመቅረፅ በግብዓትነት የሚያገለግሉ የምርምር ውጤቶችን ማቅረብ ነው፡፡

1.3.2. የጥናቱ ዝርዝር ዓላማዎች

ይህ ጥናት በዋናነት የሚከተሉትን ዝርዝር ዓላማዎች ያካትታል፡-

- በሀገር አቀፍ ደረጃ ዜጎች ያላቸዉን ጥቅል የሳይበር ደህንነት እዉቀት (Knowledge) መለካት፤
- ዜጎች ስለ ሳይበር ደህንነት ያላቸውን አመለካከት (Attitude) መለካት፤
- የዜጎችን የሳይበር ቴክኖሎጅ አጠቃቀም (Practice) ደረጃ ማወቅ፤

1.4. የጥናቱ ፋይዳ

የዚህ ጥናት ውጤት በመጀመሪያ ደረጃ በኢትዮጵያ ያለው አጠቃላይ የዜጎች የሳይበር ደህንነት ንቃት ሕሊና በምን ያህል ደረጃ ላይ እንደሚገኝ ለማወቅና በቀጣይም በየጊዜው የሚኖረውን ዕድገትና ለውጥ ለመገንዘብ መሠረታዊ የመረጃ ምንጭ እንዲኖር ያስችላል፡፡

3 የኢንፎርሜሽን መረብ ደህንነት አስተዳደር

በሁለተኛ ደረጃ ጥናቱ ኢመደአ በተለያዩ የሚዲያ አማራጮችና በሌሎችም መንገዶች እያከናወናቸው ያሉትን የሳይበር ደህንነት የንቃተ ሕሊና ግንባታ ሥራዎች በተጨባጭ ምን ያህል ውጤት እያመጡለት መሆናቸውን ለማወቅ ያስችለዋል፡፡ ይህም በሃገሪቱ ያለውን የዜጎችን የሳይበር ደህንነት ንቃተ ሕሊና ደረጃ ለማወቅና ያሉትን ክፍተቶችም በትክክል ለመገንዘብ ስለሚያግዘው በቀጣይ ክፍተቶችን ለመሙላት ውጤታማ የንቃተ ሕሊና ፕሮግራሞችን ለመቅረጽ ያስችላል፡፡

ከዚህ ባሻገርም የሳይበር ደህንነት ንቃተ ሕሊናን በሚመለከት ለሌሎች ተቋማትም መሠረታዊ የመረጃ ምንጭ ሆኖ ከማገልገሉም በተጨማሪም የዚህ ጥናት ውጤት በቀጣይ በዘርፉ ለሚደረጉ ጥናትና ምርምሮችም በዋና ግብዓትነት ያገለግላል ተብሎ ይታመናል፡፡

1.5. የጥናቱ ወሰን

በፅንሰ ሃሳብ ደረጃ ጥናቱ የዜጎችን የሳይበር ደህንነት ዕውቀት፣ አመለካከትና አተገባበር ዙሪያ ያተኩራል፡፡ በዚህም ጥናቱ በመሠረታዊ መልኩ በሃገር አቀፍ ደረጃ ያለውን ብሔራዊ የሳይበር ደህንነት ንቃተ ሕሊና መረጃን መሰብሰብና የተለያዩ የሚድያ አማራጮችን ጨምሮ በቀጣይ ሊሠሩ የሚገባቸው የሳይበር ደህንነት የንቃተ ሕሊና ሥራዎችን መጠቆም ላይ አድማሱን የወሰነ ሲሆን በዚህም ጥናት “ዜጎች” ማለት የኢንተርኔት ተጠቃሚዎች ዜጎችን ይመለከታል።

የአጠናን ስልቱን በሚመለከት ጥናቱ የኢንተርኔትና የኢንፎርሜሽን ኮምዩኒኬሽን ቴክኖሎጂ ውጤቶች ተጠቃሚዎች ላይ የሚያተኩር ሲሆን በግልም ሆነ በሥራ ኢንተርኔትን ወይንም የኢንፎርሜሽን ኮምዩኒኬሽን ቴክኖሎጂ ውጤቶችን የሚጠቀሙ ዜጎች የጥናቱ አካል ናቸው፡፡
የጥናቱን ተሳታፊዎችና የተካሄደበትን ቦታ በተመለከተም ይህ ጥናት የራንደም ናሙና (Random Sampling) ስልቶችን በመጠቀም፤ በኢትዮጵያ በሁሉም ክልሎች የሚገኙ የሳይበር ቴክኖሎጅ ተጠቃሚ የሆኑ ዜጎችን በማሳተፍ፣ በተመረጡ ከተሞችና ተቋማት እንዲሁም የማህበረሰብ ክፍሎች ውስጥ የተሰበሰቡ መረጃዎችን መሰረት በማድረግ ተከናውኗል፡፡

1.6 የጥናቱ ውስንነቶች (Limitations of the study)

ይህ ሀገር አቀፍ የሳይበር ደህንነት ንቃተ ሕሊና ጥናት በዋና ዓላማው እንደተገለፀው በሁሉም የሀገራችን ክፍል ሊካሄድ ታስቦ እንደነበር የሚታወቅ ቢሆንም በሰሜኑ የሀገራችን ክፍል በነበረዉ የፀጥታ ችግር ምክንያት ከትግራይ ክልል መረጃዎችን መሰብሰብ አለመቻሉ የጥናቱ አንዱ ውስንነት ተደርጎ ይወሰዳል፡፡

በሌላ በኩል የጥናቱን አካሄድ በሚመለከት ጥናቱ ከመካሄዱ አስቀድሞ በፕሮፖዛል ደረጃ በጊዜ ዕቅድና በጀት ደረጃ ፀድቆ ወደ መረጃ መሰብሰብ ሥራ ከተገባና ከ75 በመቶ በላይ መረጃዎች ከተሰበሰቡ በኋላ ከበላይ አመራሩ በተሰጠ አዲስ አቅጣጫ መሠረት መረጃ የመሰብሰብ ሥራው በአዲስ መልክ በውጭ የመረጃ ሰብሳቢዎች አማካኝነት እንዲከናወን መደረጉ የጥናቱን የአፈፃፀም ጊዜ በከፍተኛ ሁኔታ አዘግይቶታል፡፡ የጥናቱን ውጤት ሪፖርት የማድረጊያ ጊዜውንም እንዲራዘም አድርጎታል፡፡ ይህም ሌላኛው የጥናቱ ውስንነት ተደርጎ ሊወሰድ ይገባል፡፡

ምዕራፍ ሁለት

የተዛማጅ ፅሁፎች ዳሰሳ

ይህ ምዕራፍ ከጥናቱ ርዕሰ ጉዳይና ነባራዊ ሁኔታ እንዲሁም ከጥናቱ ዓላማ ጋር ተያያዥነት ያላቸው ነጥቦችና የጥናቱን ውጤት ለማረጋገጥ የሚያስችሉ ተዛማጅ ይዘት ያላቸው የጥናት ውጤቶች ዳሰሳ የተከናወኑበት ነው፡፡

2.1 የሳይበር ደህንነት

የሳይበር ደህንነትን ፅንሰ ሀሳብ ብዙ ጊዜ ከመረጃ ደህንነት ጋር በተለዋዋጪነት እንጠቀመዋለን፡፡ ይሁንና ሁለቱም ሃሳቦች የተቀራረበ የሃሳብ ይዘት ቢኖራቸውም ተመሳሳይ የሆነ ሃሳብን ግን አይገልጹም (ቮኦን ሶለሞን እና ቫን ኒክሬክ 2013)፡፡ ስለሆነም በሃሳቦቹ ላይ ግልጽ የሆነ መረዳትን ለመፍጠር ሲባል የሁለቱን ሃሳቦች ግልጽ ልዩነት ለማየት እንሞክራለን፡፡

ዓለም አቀፉ ተቋም ISO/IEC 27000 (2016) የመረጃ ደህንነትን፤ "የመረጃ ደህንነት ማለት የመረጃን ሚስጥራዊነት፣ ቅንጅትና የመረጃውን ተደራሽነት ማስጠበቅ" በማለት ይተረጉመዋል፡፡ ዓላማውም የመረጃ ደህንነት መሠረታውያን(CIA Triad) የሚባሉትን ሦስቱን የመረጃ መገለጫዎች፤ ማለትም ሚስጥራዊነት(-Confidentiality)፣ ምልዑነት(Integrity)፣ እና ተደራሽነት(Availability) በመጠቀም የመረጃ ደህንነትን ማስጠበቅ መሆኑን ይገልጻል፡፡ ሚስጥራዊነት(Confidentiality) አንድን መረጃ የተፈቀደላቸው ሰዎች ብቻ ማግኘት እንዲችሉ ማድረግ፣ ምዕሉነት(Integrity) መረጃዎችን በተሟላ መልኩ ሳይሰረዙ ሳይለወጡ ማግኘት እንዲችሉ ማድረግና ተደራሽነት(Accessibility) ማለት ደግሞ መረጃዎች ለተፈቀደላቸው ሰዎች በተፈለገው ጊዜና ቦታ እንዲደርሱ የማስቻል ዘዴ መሆኑንም ያብራራል፡፡ በተያያዘም እነዚህን ሦስት መሠረታዊ የመረጃ ደህንነት ማስጠበቂያ ዘዴዎች ጥቅም ላይ ማዋል ሳይቻል ሲቀር የመረጃ ደህንነት ውድቀት ይፈጠራል ወይንም መረጃው ደህንነቱ ያልተጠበቀ ይሆናል ማለት ነው፡፡

በሌላ በኩል እንደ ጃንግ (2011) ገለጻ የሳይበር ደህንነት ማለት መረጃዎችን፤ የኮሚውንኬሽን ኔትወርኮችን በሳይበር ምህዳሩ ላይ ሊደርሱ ከሚችሉ የሳይበር ጥቃቶች/የሳይበር ተጋላጭነቶች መከላከል ነው ሲል ይገልጸዋል፡፡ የአለማቀፍ የቴሌኮሚንኬሽን ጥምረት (ITU) በ2008 ባወጣው የጥናት ሪፖርት መሰረት የሳይበር ደህንነት ማለት የቴክኖሎጂ ቁሳቁሶች፣ ፖሊሲዎች፣ የደህንነት ሃሳቦች፣ የደህንነት ማስጠበቂያዎች፣ መመሪያዎች፣ የስጋት ማኔጅመንት መመሪያዎች፣ ተግባሮች፣ ስልጠናዎች፣ ምርጥ ተሞክሮዎች፣ ማስጠበቂያዎችና ቴክኖሎጂዎችን ያካተተ ሆኖ የሳይበር ምህዳሩን፣ የተቋማትንና የተጠቃሚዎችን የመረጃ ሃብቶች ከሳይበር ጥቃት ለመከላከል የሚጠቀሙበት ስርዓት እንደሆነ ያሳያል፡፡ ይህ ትርጉም የሳይበር ደህንነት ባህሪያትን የያዘና ጥበቃ የሚደረግላቸውን አካላት አካቶ የያዘ ነው፡፡ የመረጃና የሳይበር ደህንነትን የሚያመሳስላቸው ሃሳብ የሁለቱም ሃሳቦች አላማ የደህንነት ባህሪ የሆኑትን ሚስጥራዊነትን፣ ቅንጅታዊነት እና ተደራሽነትን (CIA triads) ማስጠበቅ መሆኑ ነው፡፡ አያይዞም ጥናቱ ቴክኒካልና ቴክኒካል ያልሆኑ

ሃሳቦችን በመግለጽ የኢንተርኔት ተደራሽነት በመስፋፋቱ ምክንያት የሳይበር ደህንነት የምንለው ሃሳብ የተለዩ መገለጫዎች እንዲኖሩት እንዳደረገውም ይገልጻል፤ እነዚህም መገለጫዎቹ የሚከተሉት ናቸው፡፡ የመረጃ ደህንነት በተናጠል ትኩረት የሚያደርገው መረጃዎች ላይ ሲሆን የሳይበር ደህንነት ደግሞ በዋናነት አለማቀፋዊ የሆኑ ስጋቶችን የሚከላከል ይሆናል፤ ይህም የስልጣን ወሰን ልዩነትን ይፈጥራል፡፡ የሳይበር ደህንነት የሚወዳደረው ከበይነ መረብ ባህሪያቶችና አዳዲስ ፈጣራዎች ጋር ስለሆነ የአጥቂዎችን ባህሪና የማጥቂያ መንገድ ማወቅ በጣም አዳጋች ያደርገዋል (ITU 2011)፡፡

የሳይበር ደህንነት መገለጫዎች ከላይ በተጠቀሱት ምክንያቶች ሳቢያ የተለያዩ ውስብስብ ችግሮችን ያስተናግዳል ዋናዎቹም የሥልጣን ወሰን እርግጠኝነት ችግር፣ አለማቀፋዊ ስጋቶችና የስጋቶች ባህሪና አይነት ችግሮችን ያስተናግዳል፡፡ ሌላው የሁለቱ ሃሳቦች ልዩነት የጥበቃ ወሰንን መሰረት ያደረገ ነው ማለትም የሳይበር ደህንነት የጥበቃ ከለላው የሰው ልጅን (የቴክኖሎጂ ተጠቃሚውን)፣ ማህበረሰቡን እንዲሁም የተጠቃሚውንና የማህበረሰቡን የመረጃ ሃብቶች የጥበቃ ከለላው ውስጥ የሚያስገባ ሲሆን የመረጃ ደህንነት ግን የመረጃ ሃብቶችን ብቻ የጥበቃ ከለላው ውስጥ በማስገባት ላይ የተመሰረተ ፅንሰ ሃሳብ ነው፡፡ ከዚህ በመነሳት የሳይበር ደህንነት ፅንሰ ሃሳብ የኢንፎርሜሽን ቴክኖሎጂ በሰዎች ላይ የሚያሳድረውን ተፅዕኖ ከግምት ውስጥ እንደሚያስገባ ማወቅ እንችላለን ስለሆነም የሳይበር ደህንነት ሃሳብ የማህበራዊና የህግ ፅንሰ ሃሳቦችን ከግምት ውስጥ በማስገባት የሳይበር ስጋቶችና የሳይበር ጥቃቶች ላይ ይሰራል፤ በተቃራኒው ግን መረጃ ደህንነት በተያያዥ ሃሳቦች ላይ ትኩረት አያደርግም ስለሆነም የሳይበር ደህንነት ፅንሰ ሃሳብ ከመረጃ ደህንነት ፅንሰ ሃሳብ በላቀ ሁኔታ ሰፊና ተያያዥነት ያላቸው ብዙ ሃሳቦችን ያጠቃለለ እንደሆነ እንረዳለን (ሳፋ እና ሌሎች 2016)፡፡

2.2 የሳይበር ደህንነት ስጋቶችና የሣይበር ጥቃት

2.2.1 የአደጋ ፅንሰ ሃሳብ

በዓለማችን ሁለንተናዊ እንቅስቃሴ በሰው ልጆች የኑሮ ሂደት ውስጥ በተደጋጋሚ ጥቅም ላይ ሲውሉ ከሚሰሙ ቃላት መካከል አደጋ ከቀዳሚዎቹ ተርታ የሚሰለፍ ነው፡፡ ከዚሁ ጋር በተያያዘ ሁሉም የሰው ልጆች እንቅስቃሴ ከአደጋ ስጋት ውጭ ሊሆን የማይችልበት ሁኔታ መኖሩም ይታወቃል፡፡ የቴክኖሎጂ ዕድገትና ውስብስብነት ደግሞ በሰው ልጆች የኑሮና የሥራ ሁኔታዎች ላይ በርካታ ኢ-ተገማች ክስተቶች እንዲበዙ አድርጓል፡፡

ብሮድዚክ በአውሮፓውያኑ አቆጣጠር 2005 ባሳተመውና (Risk,Crisis and Security Management) የሚል መጠሪያን በሰጠው መጽሐፉ፤ ስጋትና ኢ-ተገማች ክስተቶችን በሚመለከት የሚነሱ ፅንሰ ሃሳቦች በቀላሉ ለመረዳት አስቸጋሪ መሆናቸውን ይገልጻል፡፡

አደጋ ለሚለው ጽንሰ ሃሳብም፡-

- ያልተፈለጉ ክስተቶች የመከሰት አጋጣሚ፤
- የተለየ ክብደትና ገፅታ ያላቸው የማይፈለጉ ክስተቶች ድምር ውጤት ፤ የሚሉና ሌሎች ተቀራራቢ ትርጉሞችን ይሰጠዋል፡፡

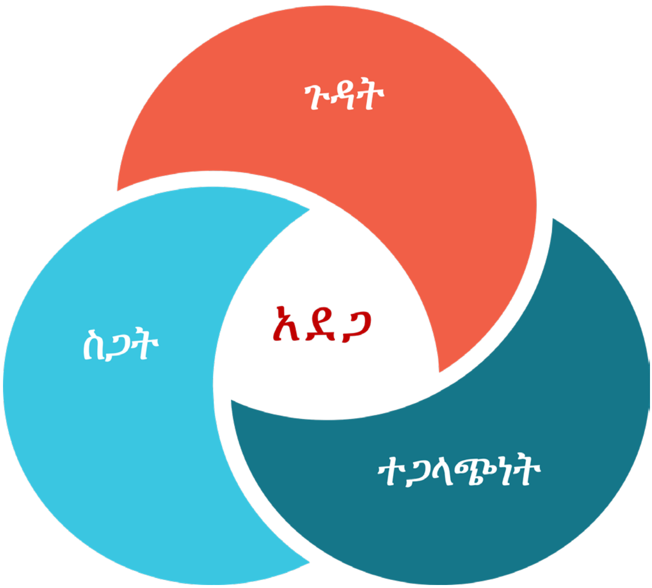
ከዚህ በተጨማሪም አደጋን ከመረዳት አኳያ ያሉ ሁኔታዎችን ሰፋ ባለ መልኩ በጥልቀት ለመመልከት ስንነሳ ሦስት የተለያዩ የእሳቤ ዓይነቶችን እናገኛለን፡፡ እነርሱም፡-

- የእውነታዊ ዓተያይ መንገድ (Realistic Approach)፤
- የስነልቦናዊ ዓተያይ መንገድ (Psychological Approach)፤
- የማህበረሰባዊ ዓተያይ መንገዶች (Sociological Approach) ናቸው።

እውነታዊ የአደጋ አተያይ መንገድ ስጋቶች በሳይንሳዊ ዕይታ፤ ማለትም በቁሳዊ መንገድ፣ በተጨባጭ ክስተቶች መታወቅ አለባቸው የሚል የአደጋ አተያይ እሳቤ ነው፡፡ ይህም አደጋዎችን በቁጥር በመለካትና ስጋቶች መቸ እንደሚከሰቱና በምን መንገድ መከላከል እንዳለብን ለማወቅ ይረዳናል የሚል የአደጋ አረዳድን የያዘ የአደጋ እሳቤ ዓይነት ነው(ዊልስ 2007)፡፡

- አደጋ = ƒ (የአደጋ ክስተት*የሚያደርሰው ጥፋት)

በዚህ መሠረት ዊልስ የሽብርተኝነትን አደጋ በማሳያነት ተጠቅሞ አደጋን ሲያስረዳ ሦስት የማንጸሪያ ነጥቦችን ይጠቀማል፡፡ ይኸውም በእውነታዊ የአደጋ አረዳድ እሳቤ አደጋ ሦስት ነገሮችን፤ ማለትም ስጋት (Threat)፣ ተጋላጪነት (Vulnerability) እና ጉዳትን (Consequences) ይይዛል፡፡ አደጋን ሲተረጉምም ዊልስ፤ "ተጨባጭ አደጋና የአደጋ ተጋላጩነት የሚያመጡት መዘዝ ነው" ይላል፡፡ የጥቃት አደጋ ማለት ሊቆጠር የሚችልና በጥቃት ምክንያት የሚደርስ ያልተጠበቀ የዋጋ ጉዳት መሆኑንም ያብራራል፡፡የዚህ የአደጋ አተያይ ትልቁ ፋይዳም በከፍተኛ ደረጃ ጥቅም ላይ የመዋል አቅም ያለውና በተጨባጭ ሊተገበር የሚችል መሆኑንም ያስገነዝባል፡፡



ምስል 1፡ የአደጋ ትርጓሜ ፅንሰ-ሃሳብ

ሁለተኛው የአደጋ አረዳድና አተያይ እሳቤ ደግሞ የሥነልቦና አተያይ የሚባለው ሲሆን ትኩረቱም "ሰዎች አደጋን እንዴት ነው የሚቀበሉት" የሚለው ላይ ነው፡፡ በማሕበራዊ ሳይንስ ዘርፍ (በሥነ ወንጀልና በሥነ ልቦና የትምህርት መስኮች ውስጥ የሰዎች የአደጋ አረዳድ በሰፊው ትኩረት ተሰጥቶት የሚጠናበት ዘርፍ ነው፡ ፡ በዚህ የአደጋ አረዳድ እሳቤ ስር ሁለት ተፅዕኖ ፈጣሪ ንኡስ የአደጋ አጠናን ዘዴዎች ያሉ ሲሆን፤ እነርሱም ሳይኮሜትሪክስ(Psychometrics) እና ኮግኒቲቭ(Cognitive) ስልቶች ናቸው (ብሮድዚክ 2005)፡፡
ከእነዚህ መካከል በዘርፉ ከፍተኛ ተቀባይነት ያለው የሳይኮሜትሪክስ የአደጋ ጥናት ሞዴል ትኩረት የሚያደርገው የግለሰቦችን የአደጋና ስጋት ሥነ ልቦናዊ አረዳድን መለካት ላይ ነው፡፡ በዚህም በዘርፉ ማህበራዊ፣ ፖለቲካዊና ተፈጥሯዊ እንዲሁም ሰው ሰራሽ አደጋዎችን የሰው ልጅ እንዴት እንደሚረዳቸው መለካት የሚያስችሉ ጥናቶች የተደረጉ ሲሆን፤ ሞዴሉም የሰው ልጆችን አደጋ አረዳድ በተመለከተ ሰፊና ጥልቀት ያላቸው መረጃዎችን መፍጠር የተቻለበት ነው(ሮያል ሶሳይቲ 1992)፡፡

ሁለተኛው ንዑስ ሥነ ልቦናዊ የአደጋ አረዳድ እሳቤ ሞዴል ደግሞ የሰው ልጆችን የአደጋ አረዳድ፤ ከሰዎች ልጆች ግንዛቤ (Cognitive) እና የውሳኔ አሰጣጥ ስርዓት ጋር የሚያያይዘው ዘርፍ ነው፡፡ ይህ ሞዴል ግለሰቦች መሠረተ ቢስ የሆኑ ምርጫዎችን ሊያደረጉ እንደሚችሉ ይሞግታል፡፡ "ይህም በባህሪያቸው ምክንያት (የሰዎች አደጋን የመጋፈጥ ወይንም የመሸሽ ባህሪያት) በምን ዓይነት መንገዶችና በምን ያህል ደረጃ ውሳኔውን እንደሚያሳልፉ ፍንጭ ይሰጣል፤ ለአደጋው የሚኖራቸውን አረዳድም ያመላክታል" ይላል፡፡

ሶስተኛው የአደጋ ፅንሰ ሃሳብ አረዳድ ደግሞ የማህበረሰባዊ አረዳድ ዘዴ ሲሆን፤ አደጋን ማህበራዊና ባህላዊ የሆኑ ጉዳዮችን ከግምት ውስጥ በማስገባት የሚካሄድ የአተያይ ወይም የሞዴል ፅንሰ ሃሳብ ነው፡፡ የስነ-ባህል/ማህበረሰባዊ ፅንሰ ሃሳብ የአደጋ አረዳድ የሚገለፀው ግለሰቡ በሚኖርበት የማህበረሰብ የአኗኗር መስተጋብር እንዲሁም አስተሳሰብ ነፀብራቅ ላይ ነው (ሶጆበርግ 2000)፡፡ ይህም ሲባል የግለሰቡ የአደጋ አረዳድ ከሚኖርበት የማህበራዊና ባህላዊ የአደጋ አረዳድ ዘይቤ በተጨማሪ የግለሰቡን እሴት (Values) እና እምነት (Beliefs) አስተሳሰብ ያማከለ ይሆናል (ሮያል ሶሳይቲ 1992)፡፡

አጂዘን (1991) ደቨሎፕ ባደረገዉ የቲወሪ ኦፍ ፕላንድ ቢሄቢዮር እንደሚያትተው የሰዉ ልጆች ባህሪ እና አንድን ነገር የመተግበር ዝንባሌ የተጠና እና በሰዉ ልጆች ሆን ተብሎ ታስቦበት የሚደረግ እንደሆነ ያስረዳል፡ ፡ የሰዉ ልጆች ዝንባሌ አንድን ተግባር ወይምድርጊት ለመፈፀም ያላቸዉን ተነሳሽነትም ይወስናል፡፡ የአጂዘን (1991) እይታን መሰረት በማድረግ ዝንባሌ እዉነተኛዉን የሰዉ ልጆች ባህሪ አይገልፅም ወይም አይወክልም የሚል ትችትን ቢያሥተናግድም ነገር ግን ዝንባሌ ካለ አንድን ሁኔታ የመተግበር እድልም ከፍ ይላል፡፡

የሰዉ ልጆች ዝንባሌ እና ፍላጎት (Intention) ደግሞ የሚወሰነዉ በአመለካከት (attitude) እንዲሁም የባህሪ ቁጥጥር ሂደቶችን መገንዘብ መቻል (Perceived Behavioral Control) እና በግላዊ መርህ (ubjective Norms) ሲሆን አመለካከት የምንለዉ አንድ ሰዉ ስለሚፈለገዉ ማንነት/ሁኔታ ጥሩ እና መጥፎ ጎኖችን ለይቶ መምረጥና መቀበል ያለመቀበልን ጉዳይ ይገልፃል፤ ሰብጀክቲቭ ኖርምስ ደግሞ ግላዊ ልምዶች ሆነዉ የተፈለገዉ ባህሪይ ላይ ተፅእኖ ሊያደርጉ የሚችሉ ሊሆኑ ይችላሉ፡፡ እንደ ቮርቨልጌት ቮን እና ፍሊክስ ሃውቢንገር (2015) እይታ ደግሞ ከሳይበር ደህንነት ንቃተ ህሊና ጋር ስናያይዘዉ ስለሳይበር ደህንነት የጥንቃቄ መንገዶች እና ካለመጠንቀቅ ስለሚደርሱ ጉዳቶች ጥሩ አመለካከት ያላቸዉ ሰዎች ለሳይበር ደህንነት ንቃተ-ህሊና እድገት መልካም አጋጣሚዎችን ይፈጥራሉ ማለት ይቻላል፡

2.2.2 የሳይበር ደህንነት ስጋቶች እና የስጋት ምንጮች

2.2.2.1 የስጋት ምንጮች

የሳይበር ደህንነት ስጋቶችን ጠቅለል ባለ መንገድ በሁለት ከፍለን ልናያቸው እንችላለን እነዚህም፤ ውስጣዊ እና ውጫዊ ስጋቶችን ያካትታል፡፡ በዚህ ረገድ በተቋማት ደረጃ የሚሰሩ የሳይበር ደህንነት ጥናቶች ውስጣዊ ለሆኑ ደህንነት ስጋቶች ብዙም ትኩረት አይሰጡም (ጃንግ ጃካርድ እና ንፓለ 2014)፡፡ ስለሆነም ውስጣዊ ስጋቶች የምንላቸው በተቋማት ሰራተኞች ሆን ተብለው የሚደረጉ ያልተገቡ አጠቃቀሞች ምክንያት የሚከሰቱ ናቸው (ዋርክነቲን እና ዊልሰን 2009)፡፡

ከዚህ ጋር ተያይዞ የሳይበር ደህንነት የስጋት ምንጮች የሚባሉት በዋናነት የኮበለሉ ሰራተኞች፣ የሳይበር ወንጀለኞች፣ የሽብር ቡድኖች፣ ሃክቲቪስቶች፣ የተደራጁ ወንጀል ቡድኖች እና የተቀናቃኝ ሃገር የመረጃ ሰራተኞችን ሊሆኑ ይችላሉ (ITU 2011)፡፡

በሌላ በኩል ውጫዊ ስጋቶች የምንላቸው ከሳይበር ደህንነት ቁጥጥር ስርዓቱ ውጪ የሚመጡ የስጋት አይነቶችን ነው፡፡ በመሆኑም ከውስጥ ሰራተኞች ውጭ የሆኑና የሳይበር ጥቃት የማድረስ ፍላጎትና አቅም ያላቸውን ሁሉ በዚህኛው ምድብ እንመድባቸዋለን፡፡ አይ ቢ ኤም/IBM (2014) ይፋ ባዳረገው ሪፖርት መሰረት በ2013 ዓ.ም ከተከሰቱ የሳይበር ጥቃቶች ውስጥ 56% ያህሉ በውጫዊ አጥቂዎች ምክንያት የተከሰቱ ሲሆኑ 17% የሚያክሉት ብቻ ነበሩ ከውስጣዊ አጥቂዎች ሊከሰቱ የቻሉት የሚል መረጃ እናገኛለን፡፡ ከዚህ በተጨማሪ ሪፖርቱ ይፋ እንዳደረገው በዉጫዊና ውስጣዊ የጋራ የጥቃት ምንጮች (Combinational Attack) አማካኝነት የተከሰቱ የሳይበር ጥቃቶች 22% የሚሆነውን ጥቃት የሚሸፍን ሲሆን ቀሪው 5% ደግሞ ከሳይበር ተጠቃሚው ፍላጎትና ሃሳብ ውጭ (Inadvertently) የተከሰተ ጥቃት እንደነበር ያመላክታል፡፡

የሳይበር አጥቂዎች የተለያዩ አይነት የጥቃት መገልገያዎችንና ቴክኒኮችን በመጠቀም አንድን ኮምፒውተር ለማጥቃት እንደሚችሉ ይታወቃል፡፡ ከሚጠቀሙባቸው ስልቶች ውስጥ አንዳንዶቹን ብንጠቅስ ለምሳሌ ማልዌሮች (ዋርሞች፣ ስፓይዌሮች እና ራንሰምዌሮች) የግለሰብን፣ የንግድ ተቋማትንና የመንግስት መስሪያ ቤቶችን የኮምፒውተር ሲስተሞች ለማጥቃት በስፋት ይጠቀሙባቸዋል (ጃንግ ጃካርድ እና ንፓለ 2014)፡፡ በ2016 እ.ኤ.አ ወደ 357 ሚሊዮን የማልዌር አይነቶች በተለያዩ መንገድ ለማጥቃት ግልጋሎት ላይ የዋሉ ሲሆን በጣም ከፍተኛ ቁጥሩን የሚሸፍነው የማልዌር አይነት የተሰራጨውም በኢሜል ግንኙነት አማካኝነት ነበር (ሳይማንቴክ 2017)፡፡

2.3 የሳይበር ጥቃት እና የሳይበር ጥቃት ዓይነቶች

በሳይበር ምህዳሩ ውስጥ በተደጋጋሚ የሚስተዋሉ የሳይበር ጥቃቶችንና የጥቃቶቹን አይነት እንዲሁም የአፈጻጸም ዘዴያቸውን በማወቅ እራሳችንን ከተጋላጪነት መከላከል ይቻላል፡፡ ትኩረት የሚሰጣቸውን ዋና ዋና የጥቃት አይነቶች እንደሚከተለው እንመለከታለን፡-

የአገልግሎት እቀባ ጥቃት (Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) :- ይህ የጥቃት አይነት ኮምፒውተሮቻችንን ባልተገባና በጣም ብዙ ትእዛዞችን በማዘዝ ተጠቃሚው የሚፈልገውን ግልጋሎት እንዳያገኝ የሚደረግበት ነው፡፡ ጥቃቱም የሚሰነዘረው በአጥቂዎች

ቁጥጥር ስር ባለ የማልሺስ መተግበሪያ የተጠቁ ብዛት ባላቸው ኮምፒውተሮች አማካኝነት ወደ ኮምፒውተራችን/ሲስተሞች ብዛት ያላቸውን ትእዛዞች በመላክ ለተጠቃሚው ግልጋሎት እንዳይሰጡ ማድረግ ነው፡፡

መካከለኛ ሰው (Man-in-the-Middle Attack)- ይህ ዓይነት የሳይበር ጥቃት የሚከሰተው አጥቂዎች የተለያዩ ዘዴዎችን ተጠቅመው በተጠቃሚው እና በሰርቨሩ መካከል ያለው ኔትወርክ ውስጥ መግባት ሲችሉና ተጠቃሚው የሚልካቸውንና የሚቀበላቸውን መረጃዎች በተለይም ሚስጥራዊ መረጃዎችን ማግኘት ሲችሉ የሚከሰት የጥቃት አይነት ነው፡፡

ማስገር/ፊሺንግ፡- ይህኛው የጥቃት አይነት ማህበራዊ ምህንድስናንና ቴክኒካል ማጭበርበሪያዎችን በመጠቀም የሚፈፀም ሲሆን ፣ ለኢላማዎች ከታዋቂ ድርጅት የተላኩ የሚመስሉ ኢሜሎችን በመላክ የኢላማውን መረጃዎች በማግኘት መረጃዎችን እንዲሰጥ የማድረግና ከሚላኩ ኢ-ሜሎች ጋር አብረው የሚገቡ አሳሳች ማልዌሮችንና ተንኮል አዘል አጥፊ ሶፍትዌሮችን ወደ ተጠቂው ኮምፒውተር እንዲገቡ በማድረግ የሚፈጸም የጥቃት አይነት ነው፡፡ ከዚህ ጋር በተያያዘ ስፒር ፊሽንግ ወይም ጥቃት ፈፃሚው ተጠቂዉን በጥልቀት በማጥናት ለተጠቂው ግላዊ እና አስፈላጊ የሆኑ መልክቶችን በመላክ የሚፈጸም የጥቃት አይነትንም ያካትታል፡፡

የፓስወርድ/የይለፍ ቃል/ ስርቆት፡- የይለፍ ቃል ስርቆት በተለያዩ መንገዶች ሊፈጸም ይችላል፡፡ የተጠቃሚውን የይለፍ ቃል ሲያስገባ በመመልከት፣ የተጠቃሚውን ኔትወርክ አውታረ መረብ በመበርበር ያልተመሰጠረ የይለፍ ቃል በማግኘት፣ የይለፍ ቃል ዳታቤዝ መረጃዎችን በእጅ በማስገባት፣ በመገመትና የማበራዊ ምህንድስናን በመጠቀም ሊከወን ይችላል፡፡ ይህን ጥቃት ለመከላከል ዋነኛው ዘዴ ጠንካራ የይለፍ ቃል (የቁጥር፣ የፊደላትና የምልክቶች ጥምር) የሆነ የይለፍ ቃል መጠቀም ነው፡፡ በተጨማሪም የአካውንት ተደጋጋሚ የመክፈት ሙከራን ማገድ የሚያስችለውን የአካውንት መቆለፊያ ስርዓት በመጠቀም፣ ነባሪ (Default) ፓስወርዶችን ፈጽሞ ባለመጠቀም እራሳችንን ከፓስዎርድ ስርቆት መከላከል ይችላል፡፡

የማልዌር የግብረ-እኩይ ሶፍትዌር/ የአጥፊ ሶፍትዌር ጥቃት (Malware Attack)፡- ይህኛው የጥቃት አይነት በሲስተሞቻችን ላይ ከእኛ እውቅና ውጪ በሚጫኑ አጥፊ መተግበሪያዎች አማካኝነት የሚከሰት ጥቃት ነው፡፡ እነዚህ አጥፊ መተግበሪያዎች ከሌሎች ትክክለኛ መተግበሪያዎች ጋር ተጣብቀው በመግባት፣የኢንተርኔት ግንኙነትን በመጠቀም ከአንዱ ወደ ሌላው ኮምፒውተር በመዛመት እንዲሁም ተጠቃሚው ክሊክ በሚያደረጋቸው አሳሳች የኢሜል ሊንኮች አማካኝነት ወደ ኮምፒተሮቻችን ሊጫኑ ይችላሉ፡፡ በዚህ መሰረት ብዙ አይነት ማልዌሮች ያሉ ሲሆን ከዋና ዋናዎቹ ውስጥ የሚከተሉትን መጥቀስ ይቻላል ፡፡

ቫይረስ (Viruse)፡- ቫይረሶች የማልዌር ዓይነት ሲሆኑ ከተለያዩ መተግበሪያዎች ጋር እራሳቸውን በማጣመር ወደ ኮምፒውተሮቻችን የሚገቡ ፕሮግራሞች ሲሆኑ ለሆነ የተለየ አላማ ለማስፈጽም የተሰሩ ናቸው፣ አብዛኛውን ጊዜ መረጃ ለማጋራት የምንጠቀምባቸው አይነት ፕሮግራሞችን እንደ ኢሜል የመሳሰሉትን ተጠቅመው እራሳቸውን ያባዛሉ፡፡

የትሮጃን ፈረስ (Trojan Horses)፡- ትሮጃን የሚባሉት በአስፈላጊ ፕሮግራሞችና መተግበሪያዎች እራሳቸውን ደብቀዉ የሚገቡ ሲሆኑ ለአጥቂዎች እንደመግቢያ በር (ባክ ዶር) ሆነው ሊያገለግሉ ይችላሉ በመሆኑም ከቫይረሶች የሚለዩት እራሳቸውን በራሳቸው ስለማያባዙ ብቻ ነው፡፡

ሰላይ ሶፍትዌር (Spyware):- ሰላይ ሶፍትዌር የአጥፊ ሶፍትዌር ዓይነት ሲሆን አንዴ ኮምፒውተራችን ላይ ከገባ በኋላ የተጠቃሚውን የግል መረጃዎች እየመዘገበ ለሦስተኛ ወገን የሚያስተላልፍ፤ አንዳንዴም ሌሎች ፕሮግራሞችን ከተጠቃሚው እውቅና ውጪ አውርዶ በራሱ ሊጭን የሚችል የሳይበር ጥቃት መፈጸሚያ ዘዴ ነው፡፡

ትል (Worm):- በኢሜይል አባሪዎች አማካኝነት ወደ ኮምፒውተሮቻችን የሚገቡ አጥፊ ፕሮግራሞች ወይም ሶፍትዌሮች ሲሆኑ በኮምፒውተሮች ትስስር አማካኝነት እራሳቸውን ያባዛሉ፤ ከቫይረስ የሚለያቸው ከሌሎች ተሸካሚ ፕሮግራሞች ጋር እራሳቸውን የማያጣምሩ መሆናቸው ነው፡፡

አጋች ሶፍትዌር (Ransomware):- ይህም የአጥፊ ሶፍትዌር ዓይነት ሲሆን የተጠቂውን ኮምፒውተር ሥርዓት በመቆለፍና በውስጡ ያሉትን መረጃዎች አግቶ በመያዝ፤ የተቆለፈውን ኮምፒውተር ለማስከፈትና የታገተውን መረጃ ለማግኘት አጥቂዎች ጥቃት የደረሰበትን አካል የገንዘብ ክፍያን የሚጠይቁበት የጥቃት ዓይነት ነው፡፡

የማስታወቂየ እኩይ ሶፍትዌሮችና ብቅ ባይ ማስታወቂያዎች(Adware and Pop-up Ads):- ይህኛው አይነት ማልዌር ከስፓይዌሮች ጋር የሚሰራ ሲሆን ተጠቃሚውን የበይነ-መረብ አሰሳ፣ የኦንላይን ታሪክ በድብቅ ከመረመረ በኋላ የተጠቃሚውን የቆየ አጠቃቀም መሰረት አድርጎ የተለያዩ ተዛማጂ ማስታወቂያዎችን በተደጋጋሚ በመላክ የሚያሰላችና ተጠቃሚው የሚላክለትን ማስታወቂያ በማየት ግዢ እንዲፈጽም ወይንም የተላከለትን ሊንክ በድንገት ክሊክ እንዲያደርግ የሚያሥችል የማልዌር አይነት ነው፡፡

2.4 የሳይበር ደህንነት ንቃተ-ህሊና ባህል ግንባታ (Maturity) ሞዴል

በብዙ መንገዶች ለመረዳት እንደሚቻለው የሳይበር ደህንነት ንቃተ-ህሊና ችግሮች የሚፈጠሩት በብስለት ማነስ ወይም ሂደቱን ጠብቆ ሊዳብሩ በሚችሉ የሳይበር ደህንነት ጉዳዮች ላይ የሚከሰቱ የአረዳድ፣ አተያይና የአተገባበር ክፍተቶች እንደሆነ መገንዘብ ይቻላል፡፡

ይህን ሃሳብ ጠቅለል ለማድረግ በንድፈ-ሀሳብ ደረጃ የአለማቀፉን የቴክኖሎጂ ደህንነት ተቋም (SANS) የሳይበር ደህንነት ንቃተ-ህሊና እና ባህል ግንባታ ሞዴል መግለፅ ያሥፈልጋል፡፡ ሃሳቡም በአጭሩ ሲገለፅ የሳይበር ደህንነት ንቃተ-ህሊና እና ባህል መፍጠሪያ መንገዶች መካከል በዋናነት የመዳበር ወይም (Security Awareness Maturity Model) የሚሰኘ የንቃተ-ህሊና መፍጠሪያ ሞዴልን መከተል ሲሆን ሞዴሉም አምስት ደረጃዎች አሉት፡፡ በመሆኑም ንድፈ-ሀሳቡ ከምንም ንቃተ-ህሊና ወይም ግንዛቤ አለመኖር (Non-Existent) እስከ ከፍተኛ ደረጃ ንቃተ-ህሊና (Metrics) ድረስ የሚያካትት ነው።

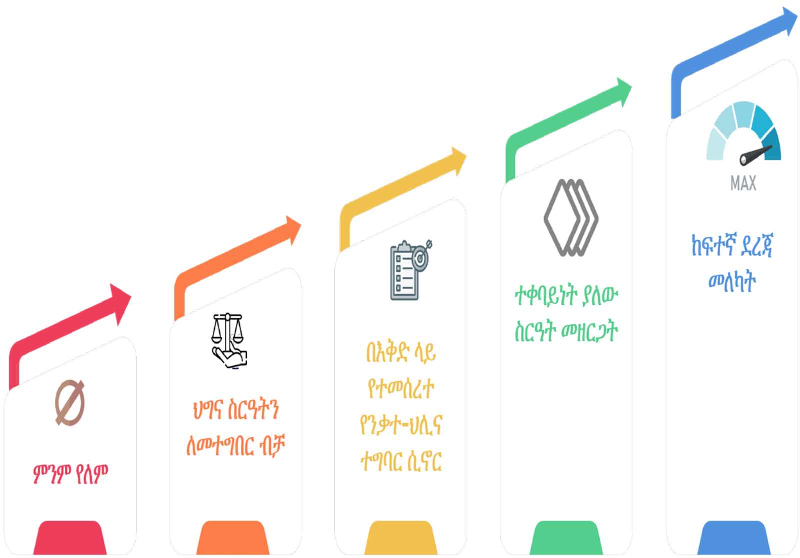
ምንም አለመኖር (No Security Awareness Program):- ይህ ደረጃ የሚገልፀው ተቋማት ምንም አይነት የሳይበር ደህንነት ስልጠና ወይም ትምህርት የማያገኙበት ዝቅተኛ ደረጃን የሚገልፅ በመሆኑ ግለሰቦች የተቋማቸውን ፖሊሲዎችና የአሰራር ሂደቶች ካለመከተላቸውም ባሻገር ራሳቸውን የጥቃት ሰለባ እንደሆኑ ወይም ሊሆኑ እንደሚችሉ አይረዱም፤

ህግና ስርዓትን ለመተግበር ብቻ (Compliance Focused):- ይህ ሃሳብ የሚያብራራው በተቋማት ደረጃ የኦዲት ወይም የተለያዩ ቅሬታ ፈጣሪ ፕሮግራሞችን መሰረት በማድረግ በሚቀርቡ ችግሮች ላይ ምላሽ ለመስጠት የሚከናወኑ ስራዎችን የሚያመላክት ሃሳብ በመሆኑ ግልፅና ጥርት ያለ የአሰራር ሂደትን ተከትሎ የሚከናዎን አይደለም፤

በእቅድ ላይ የተመሰረተ ንቃተ-ህሊና ፕሮግራም (Promoting Awareness & Change):- ይህ ክፍል የሞዴሉ የመሪ መስመር በመሆን የሚያገለግል ከመሆኑ ጋር ተያይዞ ዋና አላማውም ተፅዕኖ መፍጠርና የአመለካከት ወይም የባህርይ ለውጥ ማምጣት ነው፤ በመሆኑም ግልፅና መካተት የሚገባቸውን የሳይበር ደህንነት ንቃተ-ህሊና ሃሳቦች ወይም ርዕሶች በግልፅ በማስቀመጥ ዕቅድ ማውጣትን ይጠይቃል፤

ቀጣይነት ያለው ንቃተ-ህሊና (Long term sustainment):- ይህ ደረጃ በዋናነት የሚያጠነጥነው በለውጥና የንቃተ-ህሊና መፍጠሪያ ደረጃ የተተከሉ ፕሮግራሞችን ማጠናከር እንዲሁም የተለያዩ የንቀ-ህሊና መፍጠሪያ ቁሳቁሶችን የይዘት ክለሳ ማድረግና ሃብት በማሰባሰብ ጠንካራ ፕሮግራምመፍጠርን ይገልጻል፤

የንቃተ-ህሊናን ደረጃ መለካት (Metrics):- ይህ ሃሳብ የሞዴሉ የመጨረሻው ክፍል ከመሆኑ ጋር ተያይዞ በተለያዩ የመለኪያ መስፈርቶች የንቃተ-ህሊና ፕሮግራሙ የፈጠረውን ለውጥና አሰራር የመለካት ሂደትንያብራራል (ሳንስ ሞዴል 2018)፡፡

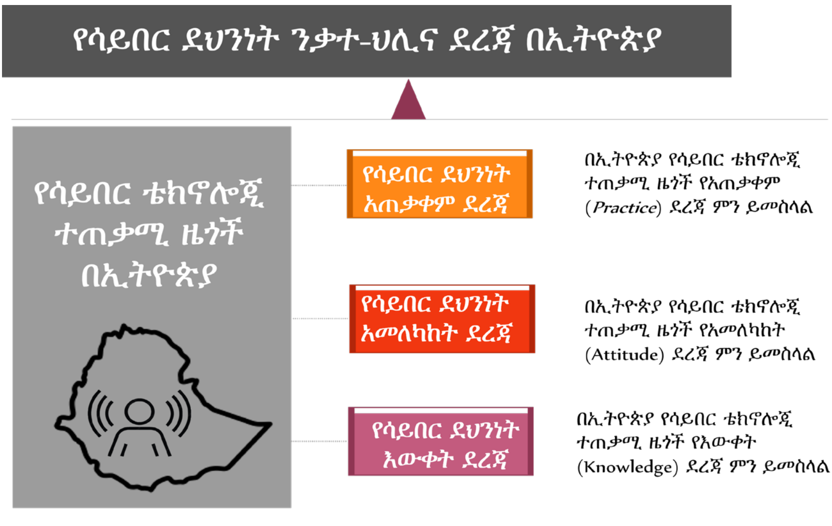


ምስል 2፡ የሳይበር ደህንነት ንቃተ ህሊና እድገት ሞዴል

2.4.1 የጥናቱ ጽነሰ-ሃሳባዊ ሞዴል (Conceptual framework)

የሳይበር ደህንነት ንቃተ-ህሊናን ለማጥናት በዋናነት ከጥናቱ ገዥ ዓላማ አንፃር ቀጥተኛ ተዛምዶ ያለው የጥናት አካሄድ ስልትን በሚመለከት ጥናቱ ሊሸፍናቸው የሚችላቸውን የመረጃ መሰብሰብያ መሳሪያዎች መጠይቅ (Questionnaire) ቅርፅ የሚያሲዝና ጠቅለል ባለ መልኩ የጥናቱን አላማ የሚገልፅና በአጭሩ ሊያብራራልን የሚችለውን የጥናት ክፍል ንድፈ-ሃሳባዊ ስልት (The highest described form of a Conceptual framework or model) በማለት ይገለፃል፡፡

ይህ የሳይበር ደህንነት ንቃተ-ህሊና ደረጃን ለመለካት የተካሄደው አገራዊ ጥናት የተከተለው የጽንሰ-ሃሳባዊ ሞዴልም (Conceptual framework) የሳይበር ደህንነት (KAP) ሞዴል የሚሰኝ ሲሆን በሳይበር ምህዳር ውስጥ ደህንነቱ የተጠበቀ የሳይበር ዓለም እንቅስቃሴንና ግንዛቤን ወይም ሞዴሉ በተለያዩ ጥናቶች ላይ የኢንፎርሜሽን/ሳይበር ደህንነት ንቃተ-ህሊናን ለማጥናት በስፋት ጥቅም ላይ የሚውል ሲሆን በይዘት ደረጃም የቴክኖሎጂውን ተጠቃሚዎች የእውቀት፣ አመለካከት እና አጠቃቀም/ባህሪ ለመለካት የተነደፈ ስልት ነው (ክሩገር እና ሌሎች 2006)፡፡ በመሆኑም ጽንሰ-ሃሳቡ በመጀመሪያ አካባቢ በእነ አልበርት ባንዱራ በሰዎች የስነ-ባህሪ ጥናት ላይ የመማማር የንድፈ-ሃሳብ አረዳድ (Theoretical orientation) በመከተል ሂደት ውስጥ ተጠኝዎች ሊያዳብሩት የሚፈለገውን ባህሪ ለመፍጠር ታስቦ የተፈጠረ ጽንሰ-ሃሳብ ሲሆን (KAP Model is primarly originated from the learning theory of Bandura (1976/7) and diffusion of innovation theory by ሮጀር (1995) cited in ኦር (2003) በውስጡም እውቀት (Aquiring knowledge)፤ አመለካከት (Generating Attitudes) እና አተገባበርን (Forming practices) በጥምረት በማካተት የተዋቀረ የአረዳድ ስልት ሲሆን ከዚህ ጥናት ነባራዊ ሁኔታ አንጻር ሞዴሉ በሚከተለው መልኩ በግልፅ ተመላክቷል፤



ምስል 3፡ የጥናቱ ጽንሰ-ሃሳባዊ ሞዴል

ምዕራፍ ሶስት

የጥናት ስነ-ዘዴ

3.1 የጥናቱ አሰራር (Research methods)

ይህ ጥናት በዋናነት የሚያተኩረዉ በኢንተርኔት ተጠቃሚ ዜጎች መካከል ያለዉን የሳይበር ደህንነት ንቃተ-ህሊና እዉቀት፣ አመለካከትና የአተገባበር ደረጃን ማወቅ ሲሆን በዚህ ክፍልም ለዚህ ጥናት የሚያስፈልጉ ሜቶዶሎጅዎችን ወይም አጠቃላይ ስልቶች ተገልፀዋል፡፡

3.2 የጥናቱ ዲዛይን (Study design)

የዚህ ጥናት ዋና አላማው የሃገራችን የኢንተርኔት ተጠቃሚ ዜጎችን የሳይበር ደህንነት ንቃተ ህሊና ደረጃ ማወቅ ሲሆን፣ ይህን አላማ ለማሳካት ጥናቱ ገላጭ (Descriptive) የጥናት ዘዴን ተጠቅሟል፡፡ ገላጭ የጥናት ስልት ጥናቱ ትኩረት የሚያደርግበትን ፅንሰ ሃሳብ ወይንም አካል በአንድ በተወሰነ ሰዓት ላይ የሚገኝበትን ሁኔታ በዝርዝር የሚገልጽ የጥናት ዘዴ ሲሆን በአብዛኛውም የገላጭ የጥናት ዘዴ ሰርቬይ (Survey) የመረጃ መሰብሰቢያ መንገድን /ስልትን ይጠቀማል (Creswell 2003)፡፡ በተጨማሪም ይህ የጥናት ዲዛይን ትክክለኛ ግኝቶችና ዉሳኔዎችን ለማሳለፍ፣ ከድምዳሜ ለመድረስ እንዲሁም መረጃዎችን በአሃዝ ለማቅረብ የሚያስችለን የጥናት ዲዛይን አይነት ነዉ፡፡

ይህ ጥናትም የሃገራችንን የኢንተርኔት ተጠቃሚ ዜጎች የሳይበር ደህንነት ንቃተ ህሊና ደረጃ ጥናቱ በሚደረግበት ወቅት ምን ያክል ነው ብሎ ለመለካት የሚከወን በመሆኑ የተጠቃሚዎችን የኢንተርኔት አጠቃቀም ልምድ እንዲሁም ባህሪ የሚገልፅ በመሆኑ ገላጭ ሰርቬይ (Descriptive Survey) የጥናት ዘዴን ተጠቅመናል፡፡

በተጨማሪም ጥናቱ ኳንቲታቲቭ የጥናት ዲዛይን (Quantitative Research Design) የተከተለ ሲሆን፣ ይህ የጥናት ዲዛይን በዋናነት በአሃዝ ሊገለፁ የሚችሉ መጠይቆችን በመጠቀም መረጃዎችን ለመሰብሰብ ይረዳናል፡፡ ስለሆነም ይህ የጥናት ዲዛይን የተለያዩ ጥንካሬዎች ያሉት ሲሆን፣ ከነዚህም መካከል ባሉት ተለዋዋጭ (Variables) መካከል ያለዉን ግንኙነት ወይም ተዛምዶ ግልጽ በሆነና ጥልቀት ባለዉ ትንተና እንዲሁም በተብራራ መንገድ ለማስቀመጥ ይጠቅመናል፡፡ በተጨማሪም መረጃን በአሃዝ የመሰብሰብ የጥናት ዲዛይን (Quantitative Research Design) ከሚያጎናፅፉቸው ጥቅሞች መካከል በዋናነት የአጥኚውን ግላዊ አመለካከት (Researchers Own Subjective Bias) በጥናቱ ሂደትና በጥናቱ ውጤት ላይ የሚኖረውን አሉታዊ ተፅዕኖ ለመቀነስ በስፋት ያግዛል፡፡ በእነዚህ ወሳኝ ምክንያቶች አማካኝነት ለጥናቱ ኳንቲታቲቭ የጥናት ዲዛይንን ተጠቅመናል፡፡

3.3 የጥናቱ ፖፑሌሽን

የዜጎች የሳይበር ደህንነት ንቃተ-ህሊና ጥናት ፖፑሌሽን ትኩረት የሚያደርገው በሀገሪቱ ዉስጥ የሚገኙትን የኢንተርኔት ተጠቃሚ ዜጎች ሲሆን፤ በዚህም መሰረት በኢትዮጵያ 22.3 ሚሊየን የኢንተርኔት ተጠቃሚዎች በ2017/18 በሀገር አቀፍ ደረጃ አሉ (ኢትዮቴሌኮም 2019) [4]፡፡ ከነዚህም ዉስጥ ለዚህ ጥናት የሚያስፈልጉትን ተቋማትና ግለሰቦችን መርጠናል፡፡

በዚህ መንገድ የዚህ ጥናት ናሙናዎች ሲመረጡ፤ የናሙና መጠንን ለመወሰን የሚያስችሉ የተለያዩ መንገዶች ቢኖሩም በዋናነት ለጥናቱ ዲዛይን ተስማሚ የሚሆን ሃብት (Resources) ማለትም የጊዜ፣ የገንዘብ እና የሰው ሃይል ውስንነት አኳያ ለጥናቱ ትክክለኛ ሊሆን የሚችለውን መንገድ መምረጥ ለጥናቱ ዓላማ መሳካት አስፈላጊ ነው በሚለው መርህ ናሙናዎች ተመርጠዋል (Cohen, Manion and Marrison 2000)፡፡

3.4 የጥናቱ ናሙና ቁጥር (Sample size)

በፕሮባቢሊቲ የናሙና መጠን ናሙናዎችን የምናገኝበትን መንገድ ለሰርቬይ ጥናት በምንጠቀምበት ወቅት Morgan and Krejcie (1970) ያዘጋጁት ሰንጠረዥ መጠቀም ጠቃሚ ይሆናል፡፡ ይህ አካሄድ የፖፑሌሽኑ ቁጥር በበዛ ቁጥር ናሙናው (Sample) አነስተኛ እንደሚሆን ያስረዳል፡፡ በዚህም መሰረት ከ100,000 እና ከዛ በላይ ለሆነ ፖፑሌሽን 384 ናሙና ተገቢ መሆኑን ይጠቁማል፡፡

በዚህም መሰረት ከእያንዳንዱ ክልል እና ከተማ መስተዳድር በህዝብ ቁጥር ብዛት መሰረት ሲኤስኤ (2007) አማካኝነት ሁሉንም የጥናቱን ተሳታፊዎች/አካላት ይወከላሉ ብለን ያሰብናቸዉን ከተሞች መርጠናል፡፡ ስለሆነም ከትግራይ ክልል (መቀሌ)፤ ከአማራ ክልል (ጎንደር፣ባህርዳር እና ደሴ)፤ ከአፋር ክልል (ሰመራ እና አሳይታ)፤ ከኦሮሚያ ክልል (አዳማ፣ጂማ እና ሻሸመኔ)፤ ከቤንሻንጉል ጉሙዝ ክልል (አሶሳ)፤ ከጋምቤላ ክልል (ጋምቤላ)፤ ከሶማሌ ክልል (ጅግጅጋ)፤ ከደቡብ ህዝቦች ክልል (ሀዋሳ እና አርባምንጭ)፤ ከሀረሪ ክልል (ሀረር) እንዲሁም ሁለቱ የከተማ አስተዳደር ከተሞችን አዲስ አበባ እና ድሬድዋን ወስደናል፡፡

በዚሁ መሰረት የናሙና መጠኑ መተማመኛ መጠን (Confidence level) 95%, እና ተቀባይነት ያለዉ የስህተት መጠን e- 0.05 (Margin of Error) ሲሆን፤ ይህን ቀመር በመጠቀም ከላይ የተገለፁት ከተሞች ባላቸዉ የህዝብ ብዛት መሰረት ከአዲስ አበባ፣ ድሬዳዋ፣ መቀሌ፣ ጎንደር፣ ባህርዳር፣ ደሴ፡ አዳማ፣ ጂማ፣ ጅግጅጋ እና ሀዋሳ ከእያንዳንዳቸዉ 384 ተሳታፊዎች እንዲሁም ሀረር እና ሻሸመኔ ከእያንዳንዳቸዉ 383 ተሳታፊዎች፣ ከአርባምንጭ 382 ተሳታፊዎች፣ ከአሶሳ እና አሳይታ ከተሞች እያንዳንዳቸዉ 378 ተሳታፊዎች ከጋምቤላ 381 እና ከሰመራ ከተማ 333 ተሳታፊዎች የተካተቱ ሲሆን፤ ነገር ግን በጥናቱ የናሙና መረጣ ዲዛይን አማካኝነት ከትግራይ ክልል መቀሌ ለዚህ ጥናት ግብዓትነት ሊሰበሰብ የነበረው መረጃ በሀገራችን ተከስቶ በነበረው የሰሜኑ ጦርነት ምክንያት ሳይሰበሰብ ቀርቷል፡፡ በመሆኑም በቀጣይ ለሚካሄዱ ሀገር አቀፍ የሳይበር ደህንነት ንቃተ-ህሊና ጥናቶች ውስጥ ልዩ ትኩረት ተሰጥቶት እንደሚሰራ ይታመናል፡፡

4 ይህ አሀዝ በዳታሪፖርታል ሪፖርት (DATAREPORTAL 2022) የዲጅታል ኢትዮጵያን በመጥቀስ እንዳመላከተው በኢትዮጵያ ወደ 29.83 ሚሊየን የኢንተርኔት ተጠቃሚዎች እንዳሉ ያሳያል፤ ይህም 25 ፐርሰንት አካባቢ ከአጠቃላይ ማህበረሰቡ ውስጥ ሽፋን እንዳለው ያመላክታል፡፡

ስለሆነም ለዚህ ጥናት ከአጠቃላይ የኢንተርኔት ተጠቃሚ ዜጎች ማለትም 22.3 ሚሊዮን ውስጥ 6458 ዜጎች ለናሙና የተመረጡ ሲሆን ከነዚህም ውስጥ 6106 መረጃዎች ተሰብስበዋል፡፡

3.4.1 የናሙና መረጣ ስትራቴጂ (Sampling strategy)

ጥናቱ አሃዛዊ መረጃዎችን ለመሰብሰብ የሚያስችለዉን ናሙና ለመምረጥ Multi-stage cluster sampling የተጠቀመ ሲሆን ይህም የተጠኝዎችን ብዛት ከምናጠናዉ የቦታ ሽፋን አንጻር እንዲሁም ከተጠኝዎች የባህሪ ልዩነት አንጻር ይህን የናሙና መረጣ ዘዴን ተጠቀምናል፡፡

ስለሆነም ከላይ በተመላከቱት የጥናቱ ዳታ መሰብሰቢያ ስፍራዎች ማለትም ከተመረጡት ከተሞች ውስጥ በአምስት (5) ክላስተሮች አማካኝነት (40% ከትምህርት ተቋማት፣ 25% የቢዝነስ ተቋማት፣ 10% ከመንግስትና የግል ቢሮዎች፣ 20% የመዝናኛ ስፍራዎች እና 5% ከመኖሪያ ስፍራዎች) መረጃዎች ተሰብስበዋል፡፡

ጥናቱ መረጃዎችን ለመሰብሰብ የሚያስችለዉን የናሙና አመራረጥ በባለብዙ ደረጃ ክላስተር ናሙና (Multi-stage cluster sampling) አማካኝነት በሚያከናውንበት ወቅት የአመራረጥ ሂደቱን በዝርዝር እንደሚከተለዉ ለማስቀመጥ ተሞክሯል፡፡

የመጀመሪያ ደረጃ፡- በሃገሪቱ የሚገኙ ዘጠኙም ክልሎችና ሁለቱ የከተማ መስተዳድሮች የተመረጡ ሲሆን በሁለተኛ ደረጃ ደግሞ በየክልሉ የሚገኙ የየክልሎቹ ዋና ዋና ከተሞችና ከፍተኛ የህዝብ ብዛት ያላቸዉ ተጨማሪ ከተሞች ተመርጠዋል፡፡

በሶስተኛ ደረጃ ከተሞች ባላቸዉ የጋራ ባህሪ መነሻ በማድረግ በአምስት ቡድኖች (Clusters) ተከፍለዋል፡፡ እነኚህም ክላስተሮች የትምህርት ተቋማት፣ የንግድ ስፍራ፣ የተቋማት ቢሮዎች፣ የመዝናኛ ስፍራዎችና የመኖርያ ስፍራ ቦታዎች ናቸዉ፡፡

በአራተኛ ደረጃ በተጠቀሱት የክልል ከተሞች ውስጥ ከተመረጡት ክላስተሮች ዉስጥ የሚገኙ ተጠኚ የትምህርት ተቋማት ዝርዝርን (Sampling Frame) ማግኘት በመቻሉ በአመንክዮ ናሙና መረጣ ሂደት (Purposive Sampling) አማካኝነት በተመረጡ ዋና ዋና ከተሞች ውስጥ የሚገኙ ዩኒቨርሲቲዎች የተመረጡ ሲሆን ከዚህ ዉጪ የሚገኙ ክላስተሮች ዝርዝር ሳምፐሊንግ ፍሬም ማግኘት ባለመቻሉ በራንደም ናሙና (Random Sampling) መምረጥ ስለማይቻል ለየክላስተሮቹ የሚመረጡ ናሙናዎች አሃዝ ተወስኗል፡፡

በዚሁ መሰረት የተመረጡት የትምህርት ተቋማት የሚከተሉት ናቸዉ፡-
ከአዲስ አበባ ከተማ አስተዳደር አዲስ አበባ ዩኒቨርሲቲ፣ ሲፒዩ የቢዝነስ እና ኮምፒዉተር ኮሌጅ፣ የካቲት 12 የመሰናዶ ትምህርት ቤት እንዲሁም ከድሬደዋ ከተማ መስተዳድር የድሬደዋ ዩኒቨርሲቲ፣ቶፕ ኮሌጅ እና ቅድስት ትሬዛ ትምህርት ቤት ተመርጠዋል፡፡

ከመቀሌ ከተማ የመቀሌ ዩኒቨርሲቲ፣ ፖሊ ኢኒስቲትዩት እና አይደር ሁለተኛ ደረጃ ትምህርት ቤት ተመርጠው የነበረ ቢሆንም በሀገራችን በነበረው ወቅታዊ ሁኔታ ምክንያት ከትግራይ ክልል ምንም ዓይነት መረጃዎችን መሰብሰብ አልተቻለም፡፡

ከጎንደር ከተማ የጎንደር ዩኒቨርሲቲ፤ ጎንደር ሜዲካል ሳይንስ ኮሌጅ እና ፋሲለደስ አጠቃላይ ሁለተኛና መሰናዶ ትምህርት ቤት እንዲሁም ከባህርዳር የባህርዳር ዩኒቨርሲቲ፣ አልካን ዩኒቨርሲቲ ኮሌጅ እና ጊዮን ሁለተኛ ደረጃ ትምህርት ቤት ተመርጠዋል፡፡

ከደሴ ከተማ የወሎ ዩኒቨርሲቲ፣ ደሴ የመምህራን ኮሌጅ እና ቅዳሜ ገበያ ሁለተኛ ደረጃ ትምህርት ቤት፤ ከሰመራ ከተማ የሰመራ ዩኒቨርሲቲ እና የሰመራ ጤና ሳይንስ ኮሌጅ፤ ከአሳይታ ከተማ የአሳይታ መምህራን ኮሌጅ እና መሀመድ ኢንፋሊን ሁለተኛ ደረጃ ትምህርት ቤት፤ ከአዳማ ከተማ የአዳማ ሳይንስና ቴክኖሎጂ ዩኒቨርሲቲ፣ የአዳማ ሆስፒታል ሜዲካል ኮሌጅ እና ሃዉሳ መሰናዶ ትምህርት ቤት፤ ከጅማ ከተማ የጅማ ዩኒቨርሲቲ፣ የጅማ መምህራን ኮሌጅ እና ጅማ ሁለተኛ እና መሰናዶ ትምህርት ቤት፤ ከሻሸመኔ ከተማ ሻሸመኔ መሰናዶ ትምህርት ቤት እና ዳዲሞስ ኮሌጅ፤ ከአሶሳ ከተማ የአሶሳ ዩኒቨርሲቲ፣ ዳንዲቦሩ የመምህራን ኮሌጅ እና አሶሳ ሁለተኛና መሰናዶ ትምህርት ቤት ተመርጠዋል፡፡

እንዲሁም ከጋምቤላ ከተማ የጋምቤላ ዩኒቨርሲቲ፣ የጋምቤላ መምህራን ኮሌጅ እና ጋምቤላ ሁለተኛና መሰናዶ ትምህርት ቤት፤ ከጅጅጋ ከተማ የጅጅጋ ዩኒቨርሲቲ እና ሼክ አብዲሰላም ሁለተኛ ደረጃ ትምህርት ቤት፤ ከሀዋሳ ከተማ የሀዋሳ ዩኒቨርሲቲ፣ የሃዋሳ አድቬንቲስት ኮሌጅ እና አዲስ ከተማ ሁለተኛ ደረጃ ት/ቤት፤ ከአርባምንጭ ከተማ የአርባምንጭ ዩኒቨርሲቲ፣ አርባምንጭ መምህራን ኮሌጅ እና አባያ ሁለተኛ ደረጃ ትምህርት ቤት፤ ከሀረር ከተማ የሀሮማያ ዩኒቨርሲቲ፣ አግሮቴክኒካል ኮሌጅ እና አቦከር ሁለተኛ ደረጃ ትምህርት ቤት ተካተዋል፡፡

3.5 የመረጃ ምንጭ (Data sources)

የጥናቱ ተቀዳሚ የመረጃ ምንጭ የሆኑት በጥናቱ ላይ የሚሳተፉ የኢንተርኔት ተጠቃሚ ግለሰቦች ሲሆኑ ለዚሁ ጥናትም መጠይቆችን (ሰርቬይ መጠይቅ) የተጠቀምን ሲሆን ሁለተኛዉ ምንጭ ደግሞ ኢጋዥ መጽሃፎችንና አርቲክሎች እንደ ወሳኝ የመረጃ ምንጭ በመሆን ለጥናቱ አገልግለዋል፡፡

3.6 የመረጃ መሰብሰቢያ መንገዶች (Data collection tools)

የጥናቱን መረጃ ተአማኒነት፣ አስተማማኝነትና ትክክለኛነት ከሚወስኑት በጣም አስፈላጊ ጉዳዮች መካከል የመረጃ መሰብሰቢያዎቹ መሳሪያዎች (Tools) ጥንካሬ የመጀመሪያ ደረጃን ይይዛል፡፡ በዚህ ጥናት የተጠቀምነው የመረጃ መሰብሰቢያ ዘዴ የፅሁፍ መጠይቅ (ሰርቬይ) ሲሆን የመጠይቁን ጥንካሬ (Reliability) ለማረጋገጥ የክሮንባች አልፋ ስታቲቲካል ልኬታን (Statistical Test) ተጠቅመናል ፡፡
በዚሁ መሰረት 0.87 አልፋ ስኮር (Cronbach's Alpha) እንደሆነ የጥናቱ መጠይቅ ስታቲስቲካል ውጤት ያሳያል፤ ይህም የመረጃ መሰብሰቢያ መጠይቁን ጥንካሬ ያመላክታል፡፡

3.7 የትንተና አካሄድ

የጥናቱን መረጃዎች ለመተንተን ቅድመ-ሁኔታዎችን ግምት ውስጥ አስገብተናል፤ ማለትም ትንተናዉን ከማካሄዳችን በፊት የተሰበሰቡ መረጃዎችን የማጣራት ስራ ለምሳሌ፡- መጠይቆች በትክክል መሞላታቸዉን

ማረጋገጥ ተገቢ ነው፡፡ በመቀጠል ኮድ ማድረግ፣ በመጨረሻም ለአሃዛዊ መረጃዎች ትንተና SPSS ሶፍትዌር በመጠቀም የመረጃ ትንተና ተሰርቷል፡፡

ትንተናዉን ለማካሄድ ዲስክሪፕቲቭ ስታትስቲክስ (Frequencies, Percentages Tables and Graphs) ተጠቅመናል፡፡ በተጨማሪም (Mean and Median) እና ኢንፈረንሻል ትንተናዎችን በተለይም ድምዳሜዎችን ለማስኬድ (To Make Conclusive Understanding) የተጠቀምን ሲሆን የጥናቱን ጥያቄዎች ለመመለስ እንዲያስችል የሚረዱ የዳታ ትንተና ስታትስቲክስ መንገዶች ተግባራዊ ተደርገዋል፡፡

3.8 የጥናት ስነ-ምግባር (Ethical Considerations)

የዚህ ጥናት ተሳታፊዎች ለጥናቱ የሰጡት መረጃዎች ለዚህ ጥናት ዓላማ ብቻ እንዲውል ተደርጓል፤ እንዲሁም መረጃ ሰጭዎቹ በጥናቱ ወረቀት ላይ በማናቸውም መልኩ ስማቸውን፣ የግል መረጃዎቻቸው እንዲጠበቅ እና እንዳይጠቀስ ከማድረግ በተጨማሪ የጥናት ዉጤቱ ሲተነተን ሚስጥራዊነትን በሚያስጠብቅ መልኩ ተከናውኗል፡፡

ምዕራፍ አራት

የመረጃ አቀራረብ፣ ትንተና እና ትርጓሜ

በዚህ ክፍል የጥናቱን ዓላማዎች ለመመለስ በሰርቬይ አማካኝነት የተሰበሰቡ መረጃዎችን መሰረት በማድረግ፤ ጥናታዊ መረጃዎች በሚከተለው መልኩ የቀረቡ ሲሆን፤ በመቀጠልም ከጥናቱ ዝርዝር ዓላማዎች አንፃር ዝርዝርና አጠቃላይ ትንታኔ ከመስራት ጎን ለጎን የትርጓሜ (Data interpretation) ስራዎች ተካሂደዋል፡፡

4.1 የስነ-ህዝብ መረጃዎች (Demographic information)

የጥናቱ ተሳታፊዎች አጠቃላይ ዲሞግራፊክ መረጃዎች ከሌሎች የጥናቱ ልኬቶች (Variables) ጋር የሚኖራቸውን ትስስር ለመለካት ይረዳ ዘንድ የፆታ፣ የዕድሜ እና የትምህርት ደረጃን የሚገልፁ መረጃዎች እንደሚከተለው ተመላክተዋል፡፡

የጥናቱ ተሳታፊዎች ዕድሜ

ዕድሜ	ድግግሞሽ	መቶኛ
14-24	3072	51.1%
25-35	2190	36.4%
36-46	565	9.4%
>47	188	3.1%

ሰንጠረዥ 1: የጥናቱ ተሳታፊዎች ዕድሜ

ከላይ እንደተመላከተው በኢትዮጵያ የኢንተርኔት ተጠቃሚ ዜጎችን ሁኔታ በሚመለከት በአብዛኛው ወጣት የሚባለው የማህበረሰብ ክፍልን የሚወክል እንደሆነ ወይም የጥናቱ ተሳታፊዎች ግማሽ ፐርሰንቱ (51.1%) ከ14-24 ዕድሜ ክልል ውስጥ የሚገኝ ሲሆን 36.4% የሚሆነው ደግሞ ከ25-35 የዕድሜ ክልል ውስጥ ይገኛል፡፡ በአጠቃላይ የጥናቱ 87.5% የሚሆነው የጥናቱ ተሳታፊዎች በአብዛኛው ወጣት የማህበረሰብ ክፍልን የሚያሳይ ሲሆን ቀሪው 12.5% የሚሆነው ደግሞ ከ36 ዓመት በላይ የዕድሜ ሽፋንን ይይዛል፡፡

የትምህርት ደረጃ

የትምህርት ደረጃ	ድግግሞሽ	መቶኛ
የመጀመሪያ ደረጃ	228	3.7%
ሁለተኛ ደረጃ	1132	18.6%
ዲፕሎማ	1607	26.4%
የመጀመሪያ ዲግሪ	2540	41.7%
ማስተርስ	494	8.1%
ፒ.ኤች.ዲ	67	1.1%
ሌላ	21	0.3%

ሰንጠረዥ 2: የጥናቱ ተሳታፊዎች የትምህርት ደረጃ

የትምህርት ዝግጅትን በሚመለከት አብዛኛው (41.7%) የጥናቱ ተሳታፊዎች የመጀመሪያ ዲግሪ ያላቸው ሲሆን ቀጥሎም ዲፕሎማ 26.4% ፐርሰንት በሁለተኛ ደረጃ ከፍተኛውን ድርሻ ይይዛል። ይህም ማለት ጥናቱ ውስጥ የተሳተፉት ተሳታፊዎች አብዛኞቹ ወይም 68.1% ያክሉ ዲፕሎማና ዲግሪ ያላቸው እንደሆነ ከማሳየቱም በላይ በኢትዮጵያ የኢንተርኔት ተጠቃሚ ዜጎች ፍሰት (Distribution) በዋናነት እዚህኛው የህብረተሰብ ክፍል ውስጥ እንደሚካተቱ ጥናቱ ይጠቁማል።

የጥናቱ ተሳታፊዎች ፆታ

ፆታ	ድግግሞሽ	መቶኛ
ወ	3959	65.10%
ሴ	2123	34.90%

ሰንጠረዥ 3: የጥናቱ ተሳታፊዎች ፆታ

ፆታን በሚመለከት በግልፅ እንደተመላከተው አብዛኛው የጥናቱ ተሳታፊዎች ማለትም 65.1% ያህሉ ወንዶች ሲሆኑ ቀሪዎቹ ደግሞ ሴቶች እንደሆኑ መረጃው ያሳያል። ይህም ማለት ጥናቱ ውስጥ የተሳተፉት አብዛኞቹ መረጃ መላሾች ከላይ ዕድሜን በሚመለከት አብዛኛዉ የሳይበር ቴክኖሎጂ ተጠቃሚ ወጣቱ የማህበረሰብ ክፍል ሲሆን የትምህርት ዝግጅትን በሚመለከት ደግሞ አብዛኛው ዲግሪና ዲፕሎማ ፕሮግራም ላይ የተካተቱት አካላት በአብዛኛው ወንዶች እንደሆኑ በመረዳት የዲሞግራፊክ መረጃዎችን ማጠቃለል ይቻላል።

4.2 የሳይበር ደህንነት እውቀት ትንተና

በዚህ ክፍል ውስጥ ከሳይበር ደህንነት ንቃተ-ህሊና መለኪያዎች ውስጥ እውቀትን በሚመለከት በኢትዮጵያ የዜጎች የንቃተ-ህሊና ደረጃ ምን ይመስላል የሚለው ሃሳብ እንደሚከተለው ቀርቧል፡-

የሳይበር ደህንነት እዉቀት መመዘኛ	እውቀት የለም	ዝቅተኛ እውቀት	መካከለኛ እውቀት	ከፍተኛ እውቀት
	%	%	%	%
የይለፍ ቃል (Password)	1.5%	66.4%	22.2%	9.8%
ጸረ-ቫይረስ (Anti-Virus)	17.3%	60.8%	16.2%	5.7%
የመተግበሪያዎች ዝመና (Software updating)	13.9%	53.5%	16.9%	15.7%
የሳይበር ጥቃት ኢንሲደንት	17.8%	49.1	15.5%	17.6%
የመረጃ ማከማቻዎች ደህንነት	12.2%	60.9%	14%	12.8%
የኮምፒዉተር ዲቫይስ ደህንነት	1%	45.5%	38.3%	15.1%
ነጻ ዋይፋይ አጠቃቀም	62.3%	0.8%	0.3%	36.6%
ዌብ ሳይት (ድረ-ገጽ)	65.2%	0.4%	0.2%	34.2%
ኮምፒዉተር ቫይረስ	78.5%	0.9%	0.9%	19.7%
ኢ-ሜይል	1.4%	75.4%	14.4%	8.8%
ማህበራዊ ሚዲያ (Social media)	35.4%	28.6%	1.1%	35%
ፊሽንግ	58.7%	0.8%	35.2%	5.4%
የሞባይል መተግሪያዎች	66%	0.9%	0.7%	32.4%
የሳይበር ጥቃት ተጋላጭነት	3.4%	47.5%	0.2%	48.9%
የሳይበር ደህንነትን ማስጠበቅ	3.8%	42.8%	0.1%	53.3%

ሰንጠረዥ 4: የሳይበር ደ/ንቃተ-ህሊና የእውቀት ትንተና

የይለፍ ቃል- ደካማ የይለፍ ቃል (Password) ምንነትንና ይዘትን በትክክል ከመረዳት አኳያ በዋናነት (12345678 የሚል ይዘት ያለው የይለፍ ቃል መጠቀም፣ የስልክ ቁጥርን መጠቀም፣ ስምንና የትውልድ ቀንን አጣምሮ መጠቀም፣ በሚወዱት ሰዉ ስም ለምሳሌ፡- በልጆች ስም ማድረግ) የሚሉትን ሃሳቦች ከግምት ውስጥ በማስገባት 89 (1.5%) እውቀት የሌላቸው፣ 3974 (66.4%) የሚሆኑት መላሾች ዝቅተኛ፣ 1329 (22.2%) መካከለኛ እንዲሁም 589 (9.8%) ከፍተኛ የሆነ የሳይበር ደህንነት እውቀት እንዳላቸው ያሳያል፡፡

ይህም ማለት የሳይበር ደህንነትን በማስጠበቅ ሂደት ውስጥ የላቀ ትኩረት ከሚሰጣቸው ፕሮቶኮሎች መካከል ደካማ የይለፍቃልን ምንነትና ባህሪያት ማወቅና ሁሌም ጠንካራ የይለፍ ቃል መጠቀምን ባህል ማድረግ አስፈላጊ ሲሆን ከላይ በዝርዝር የተገለፁት አማራጮች ደካማ የይለፍ ቃል (Password) ሁኔታን በሚመለከት ሁሉም ደካማ የይለፍ ቃልን የሚገልፁ ሃሳቦች ሲሆኑ ዉጤቱም በኢትዮጵያ የኢንተርኔት ተጠቃሚ ዜጎች በአብዛኛው ዝቅተኛ የሆነ የእውቀት ደረጃን የሚገልፅ ሲሆን በሌላ በኩል ጠንካራ የሆነ የይለፍ ቃል አጠቃቀም ክፍተትንም በግልፅ ያሳያል፡፡
ስለሆነም የሳይበር ደህንነትን ለማስጠበቅ የምንጠቀመው የይለፍ ቃል ጠንካራና በቀላሉ ሊገመት የማይችል መሆን ይኖርበታል፡፡ ይህም ማለት 12345678 በማለት መጠቀም፣ የስልክ ቁጥሮቻችንን እንደ ይለፍ ቃል መጠቀም፣ ስምንና የትውልድ ቀንን አጣምሮ መጠቀም፣ በቅርበት በሚወዷቸው ሰዎች ስም መጠቀም፤ ለምሳሌ፡-በልጆች፣በሚስት ወይም በባል፣ በእናት ወይም በአባትና የመሳሰሉትን መሰረት በማድረግ የይለፍ ቃል የመጠቀም ልምዶችን በመቅረፍ ጠንካራ የይለፍ ቃል አጠቃቀም ባህልን ማጎልበት ሲሆን በተጨማሪም ከስምንት በላይ ስብጥሮች (Characters) ያሉት እነሱም የቁጥርና የፊደላት እንዲሁም የተለያዩ ምልክቶችን የያዘ፣ ቶሎ ቶሎ የሚቀያየር እና ለተለያዩ አካውንቶች የተለያዩ የይለፍ ቃላትን የመጠቀም መርህን ይይዛል፡፡

ጸረ-ቫይረስ- ትክክል ያለሆነ የጸረ-ቫይረስ (Anti-Virus) ምንነትን በሚመለከት (ጸረ-ቫይረስ ምን እንደሆነ አለማወቅ፣ ጸረ-ቫይረሶች ያን ያህል ለሞባይሎች/ኮምፒዉተሮች አይጠቅሙም፣ ጸረ-ቫይረስ መጫን የኮምፒዉተርን/ስልክን ፍጥነት ስለሚቀንስ መጠቀሙ አያስፈልግም፣ ጸረ-ቫይረስ አንዴ ስልክ/ኮምፒዉተር ላይ ከተጫነ ያለምንም ችግር ለ1 ዓመት ያገለግላል) የሚሉ ሀሳቦች እንደ አማራጭ የቀረቡ ሲሆን፤ 1031 (17.3%) እውቀት የሌላቸው፣ 3620 (60.8%) ዝቅተኛ እውቀት፣ 964 (16.2%) መካከለኛ እውቀት እንዲሁም 337 (5.7%) ከፍተኛ እውቀት እንዳላቸው የተሰጡት ምላሾች ያመላክታሉ፡፡

በመሆኑም ትክክል ያልሆነ የፀረ-ቫይረስን ምንነትና አስፈላጊነትን ለመለካት ከላይ የተገለፁት ሃሳቦች ሁሉም ትክክል አይደሉም፡፡ በመጀመሪያ ደረጃ ጸረ-ቫይረስን አለማወቅ ብቻ ሳይሆን ለምንጠቀምባቸው የዲጅታል ቴክኖሎጂዎች የጎላ ሚና እንደሌላቸው፣ ስልኮቻችን ላይ ወይም ኮምፒዉተሮቻችን ላይ ከተጫኑ ደግሞ ፍጥነቱን እንደሚቀንሱና አንድ ጊዜ ከተጫኑ ለረጅም ጊዜ ያለማዘመን መጠቀም ሁሉም ትክክል ባለመሆናቸው በጸረ-ቫይረስ ጉዳይ በኢትዮጵያ የኢንተርኔት ተጠቃሚ ዜጎች ላይ አብዛኛው 3620 (60.8%) ዝቅተኛ የሆነ የእውቀት ደረጃን ከማሳየቱም ባሻገር ትክክለኛ የጸረ-ቫይረስ አጠቃቀም መርህን በመከተል በቀላሉ ልንከላከላቸው የምንችላቸውን የሳይበር ጥቃቶች በመጨመር የራሱ የሆነ አሉታዊ ተጽኖዎች ይኖሩታል ፡፡

በመሆኑም በዚህ የሳይበር ቴክኖሎጅ ዘመን ማንኛውም የቴክኖሎጂ ተጠቃሚ ስለ ጸረ-ቫይረስ ምንነት ማወቅ ይኖርበታል፤ በዋናነትም ህጋዊ (Licensed) የሆነ ጸረ-ቫይረስን ገዝቶ መጠቀም፣ ከታማኝ ምንጮች አውርዶ መጠቀም እንዲሁም ቶሎ ቶሎ ማዘመን አስፈላጊና ትክክለኛ የጸረ-ቫይረስ አጠቃቀም ሁኔታን

የሚገልጹ ሃሳቦች በመሆናቸው የምንጠቀምባቸውን የዲጂታል ቴክኖሎጂዎችና ተጠቃሚዎች ራሳቸውን ከሳይበር ደህንነት ስጋት ለመታደግ አስፈላጊዎች ናቸው፡፡

የመተግበሪያዎች ዝመና (Software updating)- ትክክለኛ የሆነ የሶፍትዌር ዝመና ወይም በየጊዜው ማዘመን (Timely Updating) ጠቀሜታ ጋር በተያያዘ በተሰጡት አማራጮች ላይ (ሶፍትዌር ምን እንደሆነ አለማወቅ፣ የኮምፒዉተርን፣ ሞባይልን ፍጥነት ይጨምራል፣ የኮምፒዉተርን/ሞባይልን ደህንነት ይጨምራል፣ ሶፍትዌርን ማዘመን (pdating) የኮምፒዉተርን/ሞባይልን የመግባባት ችሎታ ከፍ ሊያደርግ ይችላል) በሚሉ ሃሳቦች ላይ 830(13.9%) ምንም እውቀት የሌላቸው፣ 3192 (53.5%) ዝቅተኛ እውቀት ያላቸው፣ 1010 (16.9%) መካከለኛና ሌሎች 937 (15.7%) የሚሆኑት መላሾች ደግሞ ከፍተኛ የሆነ የእውቀት ደረጃ እንዳላቸው ውጤቱ ያመላክታል፡፡

ስለሆነም የምንጠቀምባቸውን የተለያዩ መተግበሪያዎች በየጊዜው ማዘመንን በሚመለከት የተመላከቱት ሀሳቦች ማዘመን (Updating) ምን እንደሆነ ካለማወቅ ውጭ የተገለጹት ሁሉም ትክክል ናቸው፡፡ ነገር ግን በዚሁ ሃሳብ ላይ አብዛኞች 3192 (53.5%) ያህሉ የጥናቱ መላሾች ዝቅተኛ የሆነ የእውቀት ደረጃ እንዳላቸው ያሳያል ወይም ትክክለኛ የሆነ የመተግበሪያዎችን ዝመና ምንነትና ጠቀሜታ በሚመለከት የኢትዮጵያ የኢንተርኔት ተጠቃሚ ዜጎች የእውቀት ደረጃ ዝቅተኛ እንደሆነ ይገልፃል፡፡

ስለዚህ የመተግበሪያዎችን ዝመና በሚመለከት ከምንነታቸው ጀምሮ በትክክል በማወቅ ቶሎ ቶሎ ማዘመን የምንጠቀመበትን ዲቫይስ የመግባባት ችሎታ ከፍ ከማድረግም ባሻገር ፍጥነቱን ይጨምራል በመሆኑም የዲቫይሶችን ደህንነት በማስጠበቅ ተጠቃሚዎችን ከሳይበር ጥቃት ለመከላከላል ያስችላል፡፡

የሳይበር ጥቃት ኢንሲደንት- የሳይበር ጥቃት እንደደረሰብን እንዴት ማወቅ እንደሚቻል (የሳይበር ጥቃት ምን እንደሆነ አለማወቅ፣ የይለፍ ቃሎች (Password) ባልተጠበቀ ሁኔታ መለወጥ፣ ያልታወቁ ሶፍትዌሮች ይታያሉ ወይም በድንገት መጫን፣ የፋይሎች መሰረዝ ወይም ያለተጠቃሚው ፍላጎት ይዘቶች መለወጥ፣ የሚጠቀሙበት ኮምፒዉተር በተደጋጋሚ ከበይነመረቡ (Internet) ጋር እየተገናኘ ያስቸግራል) በሚሉ አማራጮች ውስጥ 1064 (17.8%) ምንም እውቀት የሌላቸው፣ 2929 (49.1%) ዝቅተኛ፣ 923 (15.5%) መካከለኛ እንዲሁም 1051 (17.6%) ደግሞ ከፍተኛ የሳይበር ደህንነት እውቀት እንዳላቸው የሚያመላክት ሲሆን የሳይበር ጥቃት ምንነትን ካለማወቅ ውጭ ሌሎች አማራጮች በሙሉ የሳይበር ጥቃት እንደደረሰብን አመላካች ሃሳቦች ናቸው፡፡ ነገር ግን በጥናቱ የመረጃ ምላሾች መሰረት አብዛኛው 2929 (49.1%) የሚሆኑት የኢንተርኔት ተጠቃሚ ዜጎች የሳይበር ጥቃት እንደደረሰባቸው የማወቅ ደረጃቸው ዝቅተኛ እንደሆነ ያሳያል፡፡

ስለሆነም በሳይበር ምህዳር ውስጥ የሳይበር ደህንነትን ለማስጠበቅ ከሚያግዙ ወሳኝ ተግባራት መካከል የሳይበር ጥቃት ምን እንደሆነ ከማወቅ ጀምሮ ሌሎች አመላካች ጉዳዮችን ማለትም የይለፍ ቃሎቻችን በምንጠቀምበት ዲቫይስ ከተጠቃሚው ቁጥጥር ውጭ ሲለወጡ የምናስተውል ከሆነ፣ የማናቃቸው ሶፍትዌሮች በዲቫይሶቻችን ላይ በድንገት የሚጫኑ ከሆነ፣ ፋይሎች የሚጠፉብንና ድንገት የሚሰረዙብን ሲሆንና የምንጠቀምበት ዲቫይስ ከተጠቃሚው ፍላጎት ውጭ ከኢንተርኔት ስርዓቶቻችን ጋር እየተገናኘ የሚያስቸግር ከሆነ የሳይበር ጥቃት እንደደረሰብን የሚያመላክቱ ወሳኝ ሃሳቦች ናቸው፡፡

የመረጃ ማከማቻዎች ደህንነት- የተንቀሳቃሽ መረጃ ማከማቻ መሳሪያ (Removable media device like USB Flash, Memory Card, Hard Disk) ስንጠቀም ማድረግ ያሉብንን ጥንቃቄዎች ከግምት ውስጥ

በማስገባት (ስካን/Scan እያደረግን መጠቀም፣ ጠንካራ የይለፍ ቃል/Password መጠበቂያ ተግባራዊ ማድረግ፣ በተንቀሳቃሽ መረጃ ማከማቻ ላይ የተያዙ መረጃዎችን በይለፍ ቃል /Password መቆለፍ እና የተሰጡት አማራጮች መልስ አይደሉም) በሚሉ ዋና ዋና ሀሳቦች ላይ የተሰጡ ምላሾች ማለትም 728 (12.2%) ምንም እውቀት የሌላቸው፣ 3637 (60.9%) ዝቅተኛ እውቀት ያላቸው 836 (14%) መካከለኛ እውቀት ያላቸው እና 766 (12.8%) ያህሉ ደግሞ ከፍተኛ እውቀት እንዳላቸው ያመላክታል፡፡

ነገር ግን የመረጃ ማከማቻዎችን የአጠቃቀም ጥንቃቄ ጉዳይ በሚመለከት ስካን ማድረግ፣ በጠንካራ የይለፍ ቃል መቆለፍ እንዲሁም በተንቀሳቃሽ መረጃ ማከማቻዎች ውስጥ የምናስቀምጣቸውን መረጃዎች በይለፍ ቃል መቆለፍ ተገቢ የጥንቃቄ መርሆች ቢሆኑም አብዛኞቹ መላሾች ከዚህ አንጻር ዝቅተኛ የእውቀት ደረጃ እንዳላቸው ያሣያል፡፡

የኮምፒዉተር ዲቫይስ ደህንነት- የኮምፒዉተራችንን/ስልካችንን ደህንነት ለማስጠበቅ ማድረግ ስለሚገባን ጥንቃቄዎች በተመለከተ (ጠንካራ የይለፍ ቃላትን (Password) መጠቀም፣ ፈቃድ ያለዉ (Licenced) የሆነ የፀረ-ቫይረስ መከላከያ መጠቀም፣ የሚጠቀሙባቸዉን ሶፍትዌሮች/አፕሊኬሽኖች ማዘመን ወይም ሁለቱን ማለትም የይለፍ ቃልንና ፀረ- ቫይረስን መጠቀም) በሚሉ ሃሳቦች ላይ የተሰጡ ምላሾች እንደሚያሳዩት 62 (1%) በጉዳዩ ላይ እውቀት የሌላቸው፣ 2720 (45.5%) ዝቅተኛ እውቀት ያላቸው፣ 2291 (38.3%) መካከለኛ እውቀት ያላቸው እንዲሁም 903 (15.1%) ያህሉ ደግሞ ከፍተኛ የእውቀት ደረጃ እንዳላቸው ያሳያል፡፡

ስለሆነም ምንም እንኳን የኮምፒተራችንን ወይም ስልካችንን ደህንነት ለማስጠበቅ ከላይ በዝርዝር አማራጭ የተመለከቱት ሃሳቦች ተገቢነት ቢኖራቸውም አብዛኛው 2720 (45.5%) ያህሉ ምላሾች በጉዳዩ ላይ ዝቅተኛ እውቀት እንዳላቸው የሚያሳይ በመሆኑ የሳይበር ደህንነትን ለማስጠበቅ በዚህ ጉዳይ ላይ አስፈላጊውን ስልጠናና የንቃተ-ህሊና ማሻሻያዎች መደረግ ይኖርባቸዋል፡፡

ነጻ ዋይፋይ አጠቃቀም- የዋይፋይ አጠቃቀምን በሚመለከት ትክክል የሆነዉ (የሆቴሎች ዋይፋይ/Wi-Fi ከድርጅቶች ዋይፋይ ደህንነታቸዉ የተጠበቀ ነዉ፣ ነፃ ዋይፋይን መጠቀም ለመረጃ መንታፊዎች/Hackers ሊያጋልጥ ይችላል፣ ነፃ ዋይፋይ በመጠቀም እጅግ ጠቃሚ/ሚስጢራዊ መረጃዎችን መላላክ የኢንተርኔት ፍጥነቱን ስለሚጨምር መጠቀም ተመራጭ ነዉ እና ነፃ ዋይፋይ በመጠቀም የሞባይል ባንክ አገልግሎት/ Mobile Banking መጠቀም ከኢንተርኔት ወጪ ስለሚያድን መጠቀሙ ይመረጣል የሚሉት አማራጮች የተሰጡ ሲሆን በጉዳዩ ላይ አብዛኞቹ ምላሾች የሚያሳዩት እውቀት የሌላቸው 3708 (62.3%) እንደሆነና 45 (0.8%) መላሾች ደግሞ ዝቅተኛ እውቀት ፣ 20 (0.3%) መካከለኛ እና 2178 (36.6%) ያህሉ ደግሞ ከፍተኛ እውቀት እንዳላቸው ያመላክታል፡፡ በመሆኑም ትክክለኛው አማራጭ ነጻ ዋይፋይን መጠቀም ለመረጃ መንታፊዎች ሊያጋልጥ ስለሚችል ጥንቃቄ ማድረግን ያሻል የሚለው ይሆናል፡፡ ከመረጃ ሰጭዎች ምላሽ በመነሳት በኢትዮጵያ የኢንተርኔት ተጠቃሚ ዜጎች ላይ በአብዛኛው 62.3% የዋይፋይ አጠቃቀምን ወይም የነፃ የዋይፋይ አጠቃቀም እውቀት እንደሌላቸው ይገልፃል፤ በመሆኑም በጉዳዩ ላይ ሰፋፊ የንቃተ-ህሊና ስራዎች እንደሚያስፈልጉ ያሳያል፡፡

ዌብ ሳይት- ትክክለኛ ድረ-ገጽን ትክክል ካልሆኑ ከማጭበርበርያ ድረ-ገጾች እንዴት መለየት እንደሚቻል በሚመለከት (ይዘገያል፣ ፈጣን ነው፣ብዙ ምስልና ቪድዮዎች ይኖሩታል እና የድረ-ገጽ አድራሻውን (URL) በማስተዋል) እንደ አማራጭ የተቀመጡ ሲሆን 3874 (65.2%) ያህሉ ምላሽ ሰጭዎች እውቀት የሌላቸው፣

26 (0.4%) ዝቅተኛ እውቀት ያላቸው፣ 9 (0.2%) መካከለኛ እውቀት እንዲሁም 2034 (34.2%) ያህሉ ከፍተኛ እውቀት እንዳላቸው የሚያመላክት ሲሆን፤ ትክክለኛው አማራጭም የዌብሳይቱን ዩአርኤል (URL) በማየት ቢሆንም በዚህ ሀሳብ ላይ የተሰጡ ምላሾች የሚያመላክቱት በአብዛኛው 3874 (65.2%) እውቀት እንደሌላቸው ነው፡፡ ይህም ደህንነቱ የተጠበቀ የዌብ ሳይት አጠቃቀም ክፍተትን ስለሚያስከትል እንደ ሀገር ለሳይበር ደህንነት አጠባበቅ ትልቅ ስጋትን ይፈጥራል፡፡

ኮምፒተር ቫይረስ- ከኮምፒዉተር/ሞባይል ቫይረስ ጥቃት ራሳችን ለመከላከል ማድረግ የሌለብን (የዘመነ/ Updated) ፀረ-ቫይረስ መጠቀም፣ ከማናቃቸዉ አካላት የሚላኩልንን የኢሜል መልእክቶች አለመክፈት፣ በhttps የሚጀምሩ ድረ-ገጾችን አለመጠቀም፣ ብዙ የዩቲዩብ/YouTube ቪድዮዎችን መመልከት በሚሉ የሃሳብ አማራጮች መሰረት 4688 (78.5%) የሚሆኑት እውቀት የሌላቸው፣52 (0.9%) ዝቅተኛ እውቀት፣ 52(0.9%) መካከለኛ እና 1179 (19.7%) ያህሉ ምላሾች ደግሞ ከፍተኛ እውቀትን ያመላክታል፤ ነገር ግን በዚሁ ጉዳይ ላይ አብዛኛው 4688 (78.5%) ያህሉ ምላሾች ከዝቅተኛ በታች እውቀት የሌላቸው ስለሆነ ጉዳዩ በንቃተ-ህሊና ስራዎች ላይ ትልቅ ተግዳሮት እንዳለው ያመላክታል።

በመሆኑም የሳይበር ቴክኖሎጂ ተጠቃሚዎች ራሣቸውን ከኮምፒውተር/ ሞባይል ቫይረስ ለመጠበቅ በhttps የሚጀምሩ ድረ-ገጾችን አለመጠቀም ከሚለው አማራጭ ውጭ ሁሉንም ቢተገብሩ ትክክለኛ ወይም በጥናቱ አሰራር መሰረት ከፍተኛ የሆነ የእውቀት ደረጃን የሚገልፅ ይሆናል፡፡

ኢ-ሜይል- የምንጠቀመው የኢሜል (Email) አካዉንት እንዴት (Hack) ሊደረግ/ ሊሰረቅ ይችላል በሚል ሀሳብ ላይ የተሰጡ አማራጮች (ነጻ ዋይፋይ/wifi በሚጠቀም ጊዜ፣ የሚላክለትን የኢሜል መልዕክት ሁሉ የሚከፍት ከሆነ፣ በቀላሉ ሊገመት የሚችል የይለፍ ቃል/Password የሚጠቀም ከሆነ፣ የሚጠቀሙበት የስልክ/ኮምፒዉተር ኦፕሬቲንግ ሲስተም/0perating System) የድሮዉ ኦሪጂናሉ ካልሆነ) በሚል ለመለካት ተሞክሯል፤ የተሰጡት ምላሾችም 83 (1.4%) ምንም እውቀት የሌላቸው፣ 4499 (75.4%) ዝቅተኛ እውቀት ያላቸው፣ 860 (14.4%) መካከለኛ እና 527 (8.8%) ያህሉ ደግሞ ከፍተኛ እንደሆነ ያሳያል፡፡ በመሆኑም ከላይ የተቀመጡት ሁሉም አማራጮች የአንድን ሰው ኢ-ሜይል አካውንት ለመስበር ምክንያት ሊሆኑ እንደሚችሉ ቢታወቅም የጥናቱ ውጤት እንደሚያሳየው ደግሞ በጉዳዩ ላይ ዝቅተኛ የሆነ የእውቀት ደረጃ እንዳለ ያሳያል፡፡

ማህበራዊ ሚዲያ- የማህበራዊ ሚዲያ (Social Media) አካውንትን ደህንነት ለማስጠበቅ ማድረግ የሌሉብን ጉዳዮች (ለሁሉም አካውንቶች ተመሳሳይ ስም እና የይለፍ ቃል /Password መጠቀም፣ በስልካችን/ኮምፒዉተራችን የምንጠቀማቸዉን አፕሊኬሽኖች ማዘመን (Updating)፣ ከተጠቀሙ በኋላ ሎግአውት (Logout) ማድረግ እንዲሁም ማዘመንና ሎግአውት ማድረግ) የሚሉ መነሻ ሃሳቦችን መሰረት በማድረግ 2110 (35.4%) የሚሆኑት መላሾች እውቀት የሌላቸው፣ 1705 (28.6%) ዝቅተኛ፣ 64 (1.1%) መካከለኛ እና 2086 (35%) ከፍተኛ እውቀት እንዳላቸው ያሳያል፡፡

ስለሆነም የማህበራዊ ሚዲያ አካውንቶችን ደህንነት ለማስጠበቅ ማድረግ ከሌሉብን ጉዳዮች መካከል ለሁሉም አካውንቶች ተመሳሳይ የይለፍ ቃል መጠቀም የሚለውአማራጭ የሳይበር ቴክኖሎጅ ተጠቃሚዎች የማህበራዊ ሚዲያ አካውንቶቻቸውን ደህንነት ለማስጠበቅ ማድረግ ከሌሉባቸው ጉዳዮች መካከል የሚጠቀስ ሲሆን ከዚህ ውጭ የተመላከቱት ሃሳቦች በሙሉ ልክና ተገቢ ጉዳዮች ናቸው፤ ሆኖም ግን 2110 (35.4%) እውቀት የሌላቸው እንዲሁም 28.6% ያህሉ ደግሞ ዝቅተኛ በድምሩ 64% ያህሉ መላሾች በጉዳዩ ላይ ክፍተት እንዳለባቸው ያሳያል፡፡

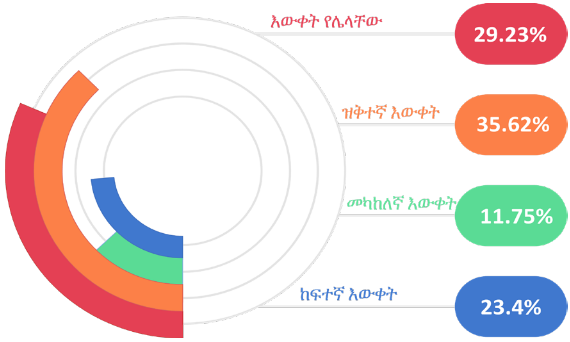
ፌሽንግ- የፊሺንግ (Phishing) ጥቃትን በሚመለከት በትክክል ሊገልጸው የሚችለው የፊሺንግ (Phishing) ጥቃት ምን እንደሆነ አለማወቅ፣ ድረገጾችን አስመስሎ በመስራት ሰው ማጭበርበር፣ ላኪው የሚፈልገው አባሪ (Attachment) በማስገባት ሎተሪ ማሸነፉን የሚገልፅ አጭር መልዕክት ስልክ ላይ መላክ እና አማራጮች መልስ ሊሆኑ አይችሉም) በሚል ለተጠየቀው ጥያቄ 3498(58.7%) እውቀት የሌላቸው፣ 46(0.8%) ዝቅተኛ እውቀት ያላቸው፣ 2097 (35.2%) መካከለኛ እና 320 (5.4%) ከፍተኛ እውቀት እንዳላቸው ምላሽ ተሰጥቷል፡፡ ስለ ፊሽንግ ጥቃትም በትክክል ከሚያሳዩት አማራጮች ውስጥ ድረ-ገፆችን አስመስሎ መስራትና ማጭበርበር እንዲሁም ሀሰተኛ የኤስ ኤም ኤስ መልዕክቶችን በመላክ ጥቃት ማድረስ የሚሉት ሲሆን የጥናቱ ውጤትም በዚህ ጉዳይ ላይ ሰፊ ክፍተት መኖሩን ማለትም 3498 (58.7%) ያህሉ እውቀት እንደሌላቸው መረዳት ይቻላል፡፡ ስለሆነም የፊሽንግ ጥቃት በኢትዮጵያ የኢንተርኔት ተጠቃሚ ዜጎች ላይ ከፍተኛ የሆነ የሳይበር ደህንነት ስጋት እንደሆነም መገንዘብ ይቻላል፡፡

የሞባይል መተግበሪያዎች- ደህንነቱ ስለተጠበቀ የሞባይል አፕሊኬሽን (Application) ትክክል ያልሆነውን አማራጭ (የአንድሮይድ/Android ስልክ አፕሊኬሽኖችን ከጎግል ፕሌይ ስቶር/Google Play Store ብቻ በማዉረድ መጠቀም፣ የአይፎን/Iphone ስልክ አፕሊኬሽኖችን ከአፕ ስቶር/App Store ብቻ አዉርዶ መጠቀም፣ ጎግል ፕሌይ ስቶር/Google Play Store እና አፕ ስቶር/App Store ላይ የሌሉ አፕሊኬሽኖችን ከጎግል ላይ ፈልጎ አዉርዶ መጠቀም እንዲሁም ሁሉም አማራጮች መልስ ይሆናሉ) በተሰኙ የመተንተኛ ሃሳቦች ላይ የተሰጠው ምላሽ 3937 (66%) እውቀት የሌላቸው፣ 56 (0.9%) ዝቅተኛ፣ 40 (0.7%) መካከለኛ እንዲሁም 1935 (32.4%) ያህሉ ደግሞ ከፍተኛ እውቀት እንዳላቸው ያሳያል፡፡ ከላይ ከተቀመጡት ሃሳቦች ውስጥም ከጉግል ፕሌይ ስቶርና ከአፕ ስቶር ፈልገን ያጣናቸውን መተግበሪያዎች ከጎግል በማውረድ መጠቀም የሚለው ትክክለኛ የሞባይል መተግበሪያዎችን ደህንነት ለማስጠበቅ የሚያግዝ አይደለም፡፡ ስለሆነም አብዛኛው 3937 (66%) ምላሾች እውቀት የሌላቸው መሆኑን እንደሚያሳየው የሞባይል መተግበሪያዎችን ደህንነት አጠባበቅ በሚመለከት ተጠቃሚዎች ላይ ሰፊ የእውቀት ክፍተት እንዳለ ለማወቅ ይቻላል፡፡

የሳይበር ጥቃት ተጋላጭነት- ለሳይበር ጥቃት ተጋላጭ የሆኑት ሀገራት እነማን ሊሆኑ እንደሚችሉ ትኩረት በማድረግ (ጀርመን እና ፈረንሳይ፣ ሱማሊያ እና ኢትዮጵያ፣ ሱዳን እና ጅቡቲ በተጨማሪም ሁሉም አማራጮች ትክክል ናቸው) ለሚለው ሃሳብ 201 (3.4%) እውቀት የሌላቸው፣ 2833 (47.5%) ዝቅተኛ፣ 11 (0.2%) መካከለኛ እና 2919 (48.9%) ደግሞ ከፍተኛ እውቀት እንዳላቸው ያመላክታል፡፡ ምንም እንኳን ሁሉም ሀገራት ለሳይበር ጥቃት ተጋላጭ እንደሆኑ የሚታወቅ ቢሆንም ከፍተኛ እውቀት ያላቸው 2919 (48.9%) ሲሆኑ 2833 (47.5%) ዝቅተኛ እውቀት እንዳላቸው ይገልፃል፤ በመሆኑም የሳይበር ጥቃት ሁሉንም ሊያጠቃ የሚችል ጉዳይ መሆኑ ሊታወቅ ይገባል፡፡

የሳይበር ደህንነትን ማስጠበቅ- የሳይበር ደህንነትን ማረጋገጥ የማን ሃላፊነት ሊሆን እንደሚችል (የመንግስት፣ የኮምፒዉተር ባለሞያዎች፣ የመከላከያ ሚኒስቴር፣ የሁሉም የጋራ ሃላፊነት) በሚሉ አማራጮች ላይ ምላሾች ተሰጥተዋል። እነዚህም 227 (3.8%) እውቀት የሌላቸው፣ 2557 (42.8%) ዝቅተኛ፣ 6 (0.1%) መካከለኛ እና 3185 (53.3%) ያህሉ ግን ከፍተኛ እንደሆነ በተሰጠው ምላሽ ይታወቃል፡፡ ምንም እንኳን የተሻለ ወይም ከፍተኛ የሚባል ምላሽ 3185 (53.3%) በዚህ ሃሳብ ላይ የተሰጠ ቢሆንም ዳሩ ግን ቀሪው 46.6% ፐርሰንት የሚያስረዳው ዝቅተኛ እውቀት እንዳለ በመሆኑ የሳይበር ደህንነትን ማረጋገጥ የሁሉም ሃላፊነት ነው የሚለውን መርህ የሚጥስ በመሆኑ ከፍተኛ የሆነ የሳይበር ደህንነት ንቃተ-ህሊና ፕሮግራሞችን የሚሻ ጉዳይ ያደርገዋል፡፡

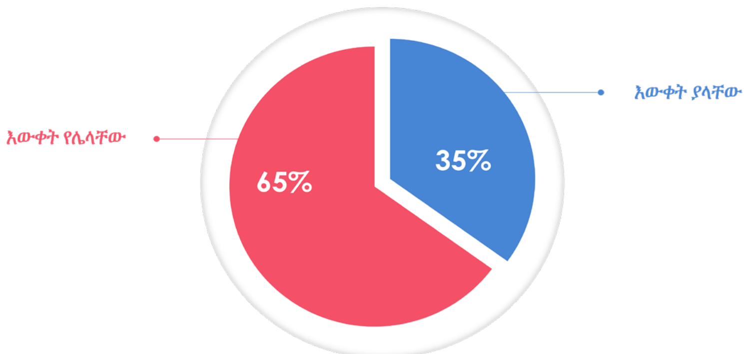
4.2.1 አጠቃላይ አማካኝ የእውቀት ደረጃ ውጤት



ግራፍ 1፡ አጠቃላይ አማካኝ የእውቀት ደረጃ ውጤት

ከላይ በግራፉ እንደተመላከተው የሳይበር ደህንነትን ለመለካት በተዘጋጁት አስራ አምስት (15) የእውቀት መጠይቆችን በመጠቀም የተገኘው አጠቃላይ ውጤት ዝቅተኛ 2126 (35.62%) እና በሁለተኛ ደረጃ ደግሞ ምንም እውቀት የሌላቸው 1742 (29.23%)፣ 1396 (23.4 %) ከፍተኛ እውቀት ያላቸው እንዲሁም 701 (11.75%) መካከለኛ እውቀት እንዳላቸው ያመላክታል፡፡

በአጠቃላይ የእውቀት ደረጃ ልኬት እውቀት የሌላቸውና ዝቅተኛ የእውቀት ደረጃን ከግምት ውስጥ በማስገባት ማለትም 3868 (64.85 %) ያህሉ የእውቀት ክፍተት ወይም እውቀት እንደሌላቸው ጥናቱ ያሳያል፡፡ በሌላ በኩል ደግሞ 2097 (35.15%) ያህሉ የጥናቱ ተሳታፊዎች የሳይበር ደህንነት እውቀት እንዳላቸው የጥናቱ አጠቃላይ የእውቀት ደረጃ ትንታኔ ያሳያል[5]፤ ይህም እንደሚከተለው በግራፍ ተመላክቷል፡-



ግራፍ 2: የሳይበር ደህንነት የእውቀት ደረጃ በኢትዮጵያ

5 የሳ/ደ እውቀት የሌላቸው ሲባል ስለሳይበር ደህንነት ምንም ዓይነት እውቀት የሌላቸው ወይም ሊከሰቱ ስለሚችሉ የሳይበር ጥቃቶች መሰረታዊ ሊባል የሚችል የሳይበር ደህንነት ማስጠበቂያ እውቀት የሌለቸው ማለት ሲሆን የሳ/ደ እውቀት አላቸው የሚባለው ደግሞ ጥናቱ የሳይበር ደህንነት የእውቀት ደረጃን ለመለካት በተጠቀማቸው 15 ጥያቄዎች ላይ ቢያንስ መሰረታዊ የሳ/ደህንነት እውቀት ያላቸውን ነው፡፡

4.3 የሳይበር ደህንነት አመለካከት (Attitude) ትንተና

ይህ የትንተና ክፍል ደግሞ በዋናነት የሚያትተው የሳይበር ተጠቃሚ ዜጎችን ንቃተ-ህሊና በሚመለከት ከእውቀት በተጨማሪ የተጠቃሚዎች ነባራዊ አመለካከት ምን እንደሚመስል ከተሰጡ የመረጃ ምላሾች በመነሳት፤ የሳይበር ደህንነት ንቃተ-ህሊና ደረጃን መለካት ይሆናል፤ ይህም እንደሚከተለው ቀርቧል፡፡

የሳይበር ደህንነት አመለካከት መመዘኛ	በጣም እስማማለሁ	እስማማለሁ	ምንም ማለት አልችልም	አልስማማም	በጣም አልስማማም
	መቶኛ	መቶኛ	መቶኛ	መቶኛ	መቶኛ
ረጅምና ዉስብስብ የሆኑ የይለፍ ቃሎችን (Passwords) ለማስታወስ አስቸጋሪ ስለሚሆኑ በቀላሉ ለማስታወስ ቀላል የሆኑ ይለፍ ቃል መጠቀም ይሻላል	32.3	32	9	17.4	9.3
ማንኛዉንም ፀረ-ቫይረስ(Antivirus) ከጓደኞቼ/ ከማንኛዉም ሌላ ቦታ ወስጄ ብጠቀም ለአመታት የስልኬን/ኮምፒዉተሬን ደህንነት ያስጠብቅልኛል (ከሃከሮች ይከላከልልኛል)	15.8	27.3	16.5	28.7	11.7
የምጠቀምባቸዉን ስልክ/ኮምፒዉተር ኦፕሬቲንግ ሲስተም (ዊንዶዉስ፣ አንድሮይድ፣IOSወዘተ.)ማዘመን(Update) ማድረግ ግዜን ስለሚወስድ በተጨማሪም ለኢንተርኔት ገንዘብ ስለሚያስወጣ ብዙም ለማዘመን ትኩረት አልሰጥም	14.7	25	15.8	29.6	14.9
ነጻ የህዝብ ዋይፋይ(i-Fi) ፈጣንና ክፍያን የሚጠይቅ ስላልሆነ የባንክ ሂሳብ ዝዉዉሮችን ጨምሮ ለማንኛዉም አገልግሎቶች ለመጠቀም ይመቸኛል	23.9	29.9	18	18.4	9.8
በሀከሮች/መረጃ መንታፊዎች/ መረጃችን መሰረቃችን ስለማይቀር በየግዜዉ የይለፍ ቃሎችን (Password) መቀየርም ሆነ ሌሎች አሰልቺ ጥንቃቄዎችን ማድረግ ግዜን ማባከን ነዉ	13.5	18.3	15.5	33.5	19.2
ያን ያህል ሚስጢራዊና እጅግ ጠቃሚ መረጃዎች በኮምፒዉተሬ/ስልኬ ስላልያዝኩ የመረጃ መንታፊዎች (Hackers) ኢላማ ልሆን አልችልም	16.4	24.5	19.1	28.9	11.2

ጓደኞቼም ሆኑ ለኔ ቅርብ የሆኑ ሰዎች ምንም አይነት ማልዌየስ ወይም ስካም (ለጥቃት የሚያጋልጠኝን መልዕክት) በኢሜል አይልኩልኝም ብየ አምናለሁ	17.4	25.9	21.4	24.8	10.5
የተለያዩ ፊልሞችን፣ ሙዚቃዎችን፣ ድራማዎችን፣ አፕሊኬሽኖችን፣ ሶፍትዌሮችን ከማንኛዉም ነጻ ድረ-ገጽ አዉርዶ መጠቀም ችግር የለዉም	15.5	25	16.2	30.1	13.1
የሶሻል ሚድያ አካዎንቶቼን ደህንነት ለማስጠበቅ (እንዳይሰረቁ ለመከላከል) ጠንካራ ፓስወርድ መጠቀም፣ ከትክክለኛ ምንጭ የወረደ፣ የዘመነ (Updated) ጸረ-ቫይረስ መጠቀም እና ዘርፈ-ብዙ ማረጋገጫ መጠቀም ያን ያህል ጥቃትን አይከላከልልኝም	13.4	20.5	17.2	32.8	16
በማህበራዊ ሚድያ የሚለቀቁ መረጃዎች ሁሉም ትክክለኛ ናቸዉ	8.2	9.5	12	31	39.3
ነፃ የሆኑ ሲስተሞችን፣ አፕልኬሽኖችንና አንቲ-ቫይረሶችን መጫንና መጠቀም ለደህንነት ስጋት ይሆናሉ ብየ አላስብም	14.9	23.8	17.2	30.3	13.8
ነፃ የህዝብ ዋይ-ፍይን በመጠቀም ሚስጢራዊ መረጃዎችን መለዋወጥ ለጥቃት (Hackers) ያጋልጣል	19.6	28.7	22.5	21.9	7.2

ሰንጠረዥ 5: የሳይበር ደህንነት አመለካከት ትንተና

የይለፍ ቃል አጠቃቀም አመለካከት - የሳይበር ደህንነትን ለማስጠበቅ ጠንካራ የይለፍ ቃል ከፍተኛ ሚና ይጫዋታል፡፡ የሳይበር ደህንነትን ለማረጋገጥ የተጠቃሚዎች አመለካከት አዎንታዊ አስተዋፅኦ አለው፡፡ ይሁን እንጂ 4,435 (73.3%) የሚሆኑት የጥናቱ መላሾች ረጅምና ዉስብስብ የሆኑ የይለፍ ቃሎችን ለማስታወስ አስቸጋሪ በመሆናቸው ቀላልና ማስታዎስ የሚያስችል የይለፍ ቃል መጠቀምን መልካም ነው የሚል አመለካከት አላቸው፡፡ በሌላ በኩል 1,618 (26.7%) የሚሆኑ መላሾች ጠንካራ የይለፍ ቃል ጠቃሚ ነው የሚል አመለካከት አላቸው፡፡ በመሆኑም የይለፍ ቃል ደህንነትን አስመልክቶ ከፍተኛ የአመለካከት ችግር እንዳለ ውጤቱ ያመላክታል፡፡

ከይለፍ ቃል ጋር በተያያዘ በተደረገ ምዘና 2,856 (47.3%) በመረጃ መንታፊዎች መረጃችን መሰረቃችን ስለማይቀር በየግዜዉ የይለፍ ቃሎችን (Password) መቀየርም ሆነ ሌሎች አሰልቺ ጥንቃቄዎችን ማድረግ ጊዜን ማባከን ነዉ የሚል አመለካከት ያላቸው ሲሆኑ 3,185 (52.7%) የሚሆኑ መላሾች መረጃችን

በሃከሮች እንዳይሰረቅ የይለፍ ቃልን መቀያየርና መሰል ተግባራትን ማከናዎን እንደሚገባ የሚያመላክት አመለካከት እንዳላቸው ውጤቱ አመላክቷል፡፡ ምንም እንኳ ከፍተኛ ቁጥር ያላቸው መላሾች የይለፍ ቃል በየጊዜው መቀያየርና ሌሎች ተግባራትን መከዎን መልካም እንደሆነ የሚያመላክት አመለካከት ያላቸው ቢሆኑም 47.3 በመቶ የሚሆን የአመለካከት ክፍተት በሀገር ደረጃ መኖሩ በግለሰቦች ስህተት ምክንያት ተቋማት፣ የግል ድርጅቶችና ግለሰቦች ለከፍተኛ የሳይበር ደህንነት ጥቃት ተጋላጭ ሊሆኑ ይችላሉ፡፡ ምክንያቱም የሳይበር ምህዳር ደህንነት ጉዳይ የጋራ ሃላፊነት ከመሆኑ ባሻገር የአንድ ሰው ስህተት በሀገር ደረጃ የሚዘልቅ የሳይበር ጥቃት መንስኤ የመሆን እድሉ ከፍተኛ በመሆኑ ነው፡፡ ስለሆነም የይለፍ ቃል አመለካከትን በሚመለከት እንደ ሀገር ከፍተኛ የሆነ ክፍተት እንዳለ ጥናቱ አመላክቷል፡፡

የፀረ-ቫይረስ አጠቃቀም አመለካከት- ፀረ-ቫይረስ በሳይበር ደህንነት ውስጥ ከፍተኛ ሚና አለው፡፡ የፀረ-ቫይረስ ሶፍትዌሮች በራሳቸው የደህንነት ችግር ይኖርባቸዋል፡፡ ፀረ-ቫይረስን ተመሳስለው የሚሰሩ እንደ ትሮጃን ሆርስ እና መሰል ተመሳሳይ የመረጃ ምንተፋ የሚሰሩ ሶፍትዌሮች በምህዳሩ ውስጥ ይገኛሉ፡፡

በመሆኑም የምንጠቀማቸውን ፀረ-ቫይረሶች ከታማኝ ምንጭ መውረዳቸውን፣ በየጊዜው የሚዘምኑ መሆናቸውንና ህጋዊ ሰውነት ካላቸው አካላት መገዛታቸውን ማረጋገጥ አንዱ የደህንነት ክፍል ነው፡፡ ይሁን እንጂ 3600 (59.6%) የሚሆኑ መላሾች ማንኛዉንም ፀረ-ቫይረስ (Antivirus) ከሚያውቁት ሰው እና ከሌላ ቦታ ወስዶ መጠቀም ችግር እንደሌለው ከመረጃ መንታፊዎችም ለአመታት ሊታደጋቸው እንደሚችልም በስምምነታቸው አመላክተዋል፡፡ ይህ ቁጥር ከሳይበር ምህዳር ባህሪ ጋር ሲታይ ቀላል የማይባል የአመለካከት ክፍተት እንደሆነ ያመላክታል፡፡ በሌላ በኩል 880 (40.4%) የሚሆኑ መላሾች በጉዳዩ አለመስማማታቸውን ያመላከቱ ናቸው፡፡ ይህም ለፀረ-ቫይረስ ያላቸው አመለካከት መልካምና የሳይበር ደህንነት የሚፈልገው አመለካከት እንደሆነ ውጤቱ ያመላክታል፡፡

ለማዘመኛዎች ተጠቃሚዎች ያላቸው አመለካከት- የምንጠቀማቸው ማንኛውም ዲቫይሶች ወይንም ቁሶች፤ ኦፐሬቲንግ ሲስተም እና መሰል የሲስተም ምርት አቅራቢዎች ክፍተታቸውን ለመሙላት የክፍተት ማዘመኛዎችን ይለቃሉ፡፡ ማዘመኛዎችን ተከታትሎ ማዘመን ሊደርሱ የሚችሉ ከፍተኛ የሳይበር ጥቃቶችን ለመከላከል ያስችላል፡፡ ይህን አስመልክቶ በተደረገ የአመለካከት ምዘና መሰረት 3,353 (55.5%) የሚሆኑ መላሾች የማዘመን ሂደቱ ጊዜ ስለሚወስድ እና ለማዘመኛ የሚሆን የኢንተርኔት ወጪ ስለሚጠይቅ ትኩረት አንሰጥም የሚል ምላሽ ሰጥተዋል፡፡ ይህም ከፍተኛ የአመለካከት ክፍተት በተጠቃሚዎች ዘንድ እንዳለ ያመላክታል፡፡ በሌላ በኩል 2,691 (44.5%) የሚሆኑ መላሾች ለማዘመኛዎች ከፍተኛ ትኩረት እንደሚሰጡ እና የተሻለ አመለካከት እንዳላቸው ከውጤቱ መገንዘብ ተችሏል፡፡

ይሁን እንጂ 55.5 በመቶ የአመለካከት ክፍተት በሳይበር ደህንነት ውስጥ ከፍተኛ የሆነ የሳይበር ጥቃት ተጋላጭነትን በተቋማት፣ በግለሰቦችና በሀገር ደረጃ (Cause for potential cyber-attack) መንስኤ ሊሆን እንደሚችል ውጤቱ ያመላክታል፡፡

ለነጻ የህዝብ ዋይፋይ የጥናቱ ተሳታፊዎች ያላቸው አመለካከት - ነጻ የህዝብ ዋይፋይ (Public Wi-Fi) በመጠቀም የሳይበር ምህዳርን መሰረት ያደረጉ ወንጀለኞች በርካታ ወንጀሎችን ይፈፅማሉ፡፡ የግለሰቦችን ግላዊ መረጃዎች ለመመንተፍ ነጻ የህዝብ ዋይፋይን ይጠቀማሉ፡፡ በመሆኑም ተጠቃሚዎች ነጻ የህዝብ

ዋይፋይ መጠቀም ለሳይበር ጥቃት ተጋላጭ መሆናቸውን የሚለካ የአመለካከት ምዘና ተከናውኗል፡፡ በመሆኑም 4,334 (71.8%) የሚሆኑ መላሾች ነጻ የህዝብ ዋይፋይ(Wi-Fi) ፈጣንና ክፍያን የሚጠይቅ ስላልሆነ የባንክ ሂሳብ ዝዉዉሮችን ጨምሮ ለማንኛዉም አገልግሎቶች ለመጠቀም ይመቻል የሚል ምላሽን ሰጥተዋል፡፡

ይህም በተጠቃሚዎች ዘንድ ከፍተኛ የሳይበር ደህንነት አመለካከት ክፍተት እንዳላቸው አመላካች ነው፡፡ በሌላ በኩል 1,702 (28.2%) የሚሆኑ መላሾች ነጻ የህዝብ ዋይፋይ መጠቀም ችግር እንዳለው በምላሻቸው አመላክተዋል፡፡ ይህም ከፍተኛ ቁጥር ያላቸው መላሾች ዝቅተኛ አመለካከት እንዳላቸው ያመላክታል፡፡ በመሆኑም ነጻ የህዝብ ዋይፋይን መሰረት ያደረጉ ጥቃቶች ቢሰነዘሩ እንደ ሃገር ከፍተኛ ጉዳት ሊያስከትል ይችላል፡፡

ነፃ የህዝብ ዋይ-ፍይን መጠቀም ለሳይበር ደህንነት መጣስ ምክንያት ከሚሆኑ ጉዳዮች አንዱ ነው፡፡ በነፃ የህዝብ ዋይፋይ ምክንያት ከሚደርሱ ጥቃቶች የጣልቃ ገቢ ሰው ጥቃት (Man-in-the-middle attacks)፣ ያልተመሳጠረ ኔትወርክ ጥሰት፣ የእኩይ ስርጭት (Malware distribution)፣ ተንኮል አዘል የኔትወርክ ሆትስፖቶች (Malicious hotspots) እና መሰል ጥቃቶች ወደ ተጠቃሚዎች ይሰነዘራሉ፡፡

ስለሆነም የተጠቃሚዎችን አመለካከት መሰረት በማድረግ የተከናወነው ሀገራዊ ጥናት ውጤት እንደሚያመላክተው 2,906 (48.3%) መላሾች ነፃ የህዝብ ዋይ-ፍይን መጠቀም ብሎም ሚስጢራዊ መረጃዎችን መለዋወጥ ለጥቃት (Hackers) ያጋልጣል የሚል አመለካከት እንዳላቸው አመላክተዋል፡፡ ሆኖም 3,103 (51.6%) ያህል መላሾች አለመስማማታቸውን አሳይተዋል፡፡ ምንም እንኳን ወደ ግማሽ በመቶ የሚደርሱ መላሾች ነፃ የህዝብ ዋይ-ፍይን መጠቀም ችግር እንዳለው ቢያመላክቱም 51.6 በመቶ የሚሆን የመላሾች አመለካከት በሀገር ደረጃ ሲታይ ቀላል የማይባል ክፍተት እንደሆነ ከሳይበር ደህንነት ባህሪ አንፃር መረዳት ያስችላል፡፡ በመሆኑም ከላይ ለተጠቀሱት አበይት ጥቃቶች ተጋላጭ የሚሆኑ ግለሰቦች፣ ተቋማት ብሎም እንደ ሀገር ከፍተኛ ክፍተት መኖሩን ከውጤቱ መገንዘብ ይቻላል፡፡

የጥናቱ ተሳታፊዎች ለመረጃ እና ጥቃት ያላቸው አመለካከት- በአለም ላይ ከፍተኛ የሳይበር ጥቃት ከሚከሰትባቸው መንገዶች መካከል የሰውን ልጅ ክፍተት እንደምክንያት ማንሳት ይቻላል፡፡ ከእነዚህ የሰው ልጅ ክፍተቶች መካከል ደግሞ የሳይበር ምህዳር ተዋንያን የሳይበር ደህንነትን ፅንሰ-ሃሳብ ለማስጠበቅ የቴክኖሎጅው ተጠቃሚዎች ካላቸው የመረጃ ሃብት ጋር የሚያገናኙት እይታ ወሳኝ በመሆኑ ነው፡፡ ይህም ማለት የቴክኖሎጅው ተጠቃሚዎች ለሳይበር ጥቃት ሊያጋልጥ የሚችል ጠቃሚ መረጃ የለኝም ከሚል አመለካከት አንፃር ብዙ ጥቃቶች ስለሚከሰቱ ሰዋዊ ክፍተቶች እንደ ሳይበር ጥቃት ምንጭ ተደርገው ይወሰዳሉ፡፡

በዚህ ጥናት 3,618 (60%) የሚሆኑ መላሾች ያን ያህል ሚስጢራዊ እና እጅግ ጠቃሚ መረጃዎች በኮምፒዉተሬ ወይንም ስልኬ ስላልያዝኩ የመረጃ መንታፊዎች (Hackers) ኢላማ ልሆን አልችልም የሚል አመለካከት እንዳላቸው አመላክተዋል፡፡ በሌላ በኩል 2,417 (40.1%) የሚሆኑ መላሾች የመረጃ መንታፊዎች ኢላማ እንደሚሆኑ የተገነዘቡና መልካም አመለካከት እንዳላቸው ውጤቱ ያሳያል፡፡
ይሁን እንጂ 60 በመቶ የሚሆኑ መላሾች የጥቃት ኢላማ መሆንን ካላቸው የመረጃ ሃብት አንፃር ነው የሚል ግንዛቤ እንዳላቸው የጥናቱ ውጤት ያመላክታል፡፡ ስለሆነም ከፍተኛ ቁጥር ያላቸው መላሾች ለሳይበር

ጥቃት ተጋላጭ መሆናቸውን መረዳት ይቻላል፡፡ ስለሆነም መረጃና የሳይበር ደህንነትን በተመለከተ የተገኘው ክፍተት ከፍተኛ ስራ የሚጠብቅ መሆኑን የሚያመላክት ነው፡፡

ለቅርብ ቤተሰብ እና ጓደኛ ያለ የመተማመን አመለካከት- በሳይበር ደህንነት ውስጥ መተማመን ለከፍተኛ ጥቃት ከሚያጋልጡ መንስኤዎች አንዱ ነው፡፡ በሳይበር ምህዳር ውስጥ አልቦ እምነት (Zero trust) የደህንነት ማስጠበቂያ ዋነኛ መፍትሔ ነው፡፡ በመሆኑም በዝምድና ብሎም ጓደኝነትን መሰረት ያደረገ መተማመን ለከፋ ጥቃት የሚያጋልጥ ስለሆነ የቴክኖሎጂ ተጠቃሚዎች አመለካከት በአልቦ እምነት የተቃኘ መሆን ይጠበቅበታል፡፡ ይሁን እንጂ 5,452 (64.7%) የሚሆኑ መላሾች ጓደኛ ብሎም የቅርብ ሰዎች ምንም አይነት ለጥቃት የሚያጋልጠን መልዕክት (Malicious or scam message) በኢሜል አይልኩልንም ብለው እንደሚያምኑ አመላክተዋል፡፡ በሌላ በኩል 2,125 (35.3%) የሚሆኑ መላሾች በጉዳዩ ላይ እንደማይስማሙ ውጤቱ ያሳያል፡፡ ከውጤቱ እንደምንረዳው ከፍተኛ ቁጥር ያላቸው መላሾች የቅርብ ቤተሰብን፣ ጓደኛን እንዲሁም የምናምናቸውን ሰዎች በመጠቀም ለሚደረግ የሳይበር ጥቃት ተጋላጭ የሚያደርግ አመለካከት አላቸው፡፡ ይህም የሳይበር ደህንነትን ለማስጠበቅ ከፍተኛ እንከን ስለሆነ ወደ አልቦ እምነት (Zero trust) አመለካከት እንዲዳብር ከፍተኛ ስራ የሚጠይቅ እንደሆነ መረዳት ይቻላል፡፡

ለነፃ ድረ- ገፆች ያለ አመለካከት- የሳይበር ምህዳር በሁለት ፅንፎች የተወጠረ ነው፡፡ የሳይበር ደህንነትን በሚያስጠብቁ እና የሳይበር ደህንነትን በሚጥሱ ሁለት አካላት መካከል፡፡ የሳይበር ወንጀለኞች፣ አጥቂዎች አሊያም መንታፊዎች ዘርፈ ብዙ የመረጃ፣ የገንዘብ አለፍ ሲልም መሰረተ-ልማቶችን የሚያወድሙበት ዘዴን ከሚቀይሱባቸው መንገዶች አንዱ በነፃ ድረ-ገፆች የሚደረግ የተንኮል አዘል ሊንኮችን መጠቀም ነው፡፡

በመሆኑም ተጠቃሚዎች ማንኛውንም የሚፈልጉትን ነገር በነፃ በሚያዎርዱባቸው ድረ-ገፆች የተለያዩ ማልዌሮችን ከጀርባ በመለጠፍ የሚፈልጉትን ኢላማ ያሳካሉ፡፡ ስለሆነም ማንኛውም ተጠቃሚ በነፃ ድረ-ገፆች ለሚያወርዷቸው ነገሮች ከፍተኛ ጥንቃቄ ብሎም እስካለመጠቀም የሚዘልቅ ተግባርን መከዎን ይገባል፡፡

ይህን መሰረት ያደረገው የአመለካከት መመዘኛ ውጤት እንደሚያመላክተው 3,423 (56.7%) የሚሆኑ መላሾች የተለያዩ ፊልሞችን፣ ሙዚቃዎችን፣ ድራማዎችን፣ አፕሊኬሽኖችንና ሶፍትዌሮችን ከማንኛዉም ነፃ ድረ-ገፅ አዉርዶ መጠቀም ችግር እንደሌለው አመላክተዋል በሌላ በኩል 2,605 (43.2%) የሚሆኑ መላሾች ችግር እንዳለው በመቃረን መልሳቸውን አስቀምጠዋል፡፡

ምንም እንኳ ውጤቱ 43.2 በመቶ ያህል ቁጥር ያላቸው መላሾች ከነፃ ድረ-ገፅ ማንኛውንም ነገር አውርዶ መጠቀም ለጥቃት ሰለባ እንደሚያደርግ ቢያመላክቱም ከፍተኛውን ቁጥር ወይም 56.7 በመቶ የሚሆን የጥናቱ መላሾች ደግሞ ምንም ችግር እንደሌለው ማመላከታቸው ከፍተኛ የአመለካከት ክፍተት በሀገር ደረጃ እንዳለ አመላካች ነው፡፡ ይህም ሀገራዊ የሳይበር ደህንነትን ለማስጠበቅ ከፍተኛ ማነቆ እንደሆነ ከውጤቱ መረዳት ተችሏል፡፡

የማህበራዊ ሚዲያ አካውንት ደህንነት አመለካከት- የማህበራዊ ሚዲያ አካውንት ደህንነትን ለማስጠበቅ ጠንካራ የይለፍ ቃል፣ የዘመኑ ፀረ-ቫይረሶችን መጠቀምና ዘርፈ-ብዙ ማረጋገጫዎችን መጠቀም አስፈላጊ ነው፡፡ ይህን መሰረት በማድረግ በተደረገው የአመለካከት መመዘኛ ውጤት 3,089 (51.1%) የሚሆኑ መላሾች ጠንካራ የይለፍ ቃል፣ ከትክክለኛ ምንጭ የወረደና የዘመነ (Updated) ፀረ-ቫይረስና ዘርፈ-ብዙ

ማረጋገጫ መጠቀም የማህበራዊ ሚዲያ አካውንቶቻችንን ደህንነት አይታደግልንም የሚል አመለካከት እንዳላቸው አመላክቷል፡፡

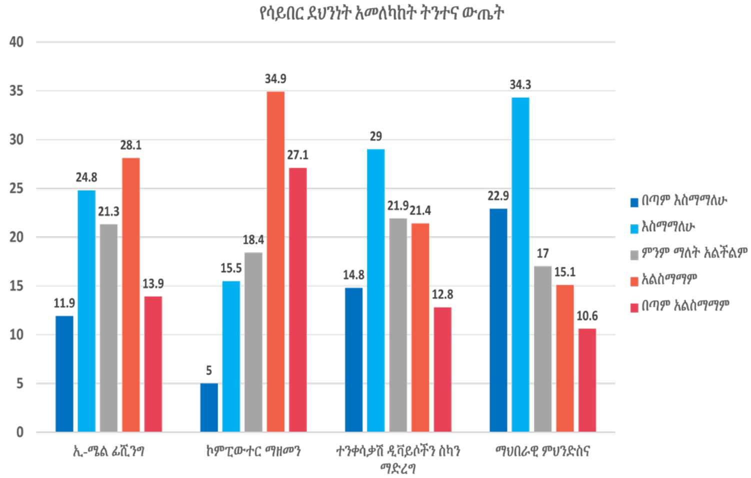
በሌላ በኩል 2,949 (48.8%) የሚሆኑ መላሾች ጠንካራ የይለፍ ቃል፣ የዘመነ ፀረ-ቫይረስና ዘርፈ-ብዙ ማረጋገጫ መጠቀም የማህበራዊ ሚዲያ አካውንቶቻቸውን ደህንነት እንደሚያስጠብቅላቸው በስምምነታቸው አመላክተዋል፡፡ ምንም እንኳ 48.8 በመቶ የሚሆኑ መላሾች መልካም አመለካከት ቢኖራቸውም 51.1 በመቶ የሚሆን የአመለካከት ችግር እንደ ሀገር መኖሩ በሳይበር ደህንነት ውስጥ ከፍተኛ ክፍተት አሊያም ስጋት ተደርጎ የሚወሰድ ነው፡፡

ማህበራዊ ሚዲያ የሰውን ልጅ የመረጃ ፍላጎት ብሎም የስነ-ተግባቦት ደረጃን ከፍ በማድረግ በማንኛውም ሰዓት የትኛውም አለም ጋር መግባባት እንዲችል አስችሎታል፡፡ ምንም እንኳ በቅፅበት ውስጥ አለም አቀፍ ተደራሽነት ያለው የማህበራዊ ሚዲያ አውታሮች የሰውን ልጅ ህይዎት በበርካታ አዎንታዊ ጎን መጥቀም ቢችልም ለሀገራት መፍረስ፣ ለሰው ልጅ እንግልት፣ ሰብዓዊ መብት መገፈፍ፣ የሀገራት የፖለቲካ ምህዳር እንዳይረጋጋ በማድረግ ብሎም የባህል መበረዝ እንዲፈጠር አለፍ ሲልም ለተቋማትና ግላዊ መረጃ ደህንነት መጠቂያ ምክንያት በመሆን በአለም ላይ ከፍተኛ ጫና እንዲፈጠር ለወንጀለኞች መደበቂያ ምሽግ በመሆን እያገለገለ ይገኛል፡፡
ስለሆነም በማህበራዊ ሚዲያ የሚለቀቁ መረጃዎች ሁሉ እውነታ የሌላቸው ብሎም የጥቃት ዒላማን ያነገቡ ሊሆኑ እንደሚችሉ መገንዘብ ያስፈልጋል፡፡ በመሆኑም በማህበራዊ ሚዲያ የሚሰራጩ መረጃዎችን አስመልክቶ በተደረገ የአመለካከት መመዘኛ ውጤት እንደሚያመላክተው 1,792 (29.7%) የሚሆኑ መላሾች በማህበራዊ ሚድያ የሚለቀቁ መረጃዎች ሁሉም ትክክለኛ ናቸዉ የሚል አመለካከት ያላቸው ሲሆን 4,236 (70.3%) የሚሆኑ መላሾች ደግሞ ሁሉም የማህበራዊ ሚዲያ መረጃዎች ትክክል አይደሉም የሚል ምላሽ ሰጥተዋል፡፡ ይሁን እንጂ 29.7 በመቶ የሚሆኑ መላሾች ሁሉም መረጃዎች ትክክል ናቸው ብለው ማመናቸው በሀገር ደረጃ ለሚፈጠር አካላዊና የሳይበር ምህዳርን መሰረት ላደረገ ወንጀል ተጋላጭ የሚያደርግ ከፍተኛ ስጋት መሆኑን መረዳት ያስችላል፡፡

የነፃ መተግበሪያዎች አመለካከት- በሳይበር ደህንነት ውስጥ ነፃ የሆኑ ሲስተሞች፣ ሶፍትዌሮች፣ አፕሊኬሽኖችና ፀረ-ቫይረሶች መጠቀም ከሶፍትዌሮች ጀርባ ለሚለጠፉ ተንኮል አዘል ማልዌሮች (እኩይ ቫይረሶች) ተጋላጭ ያደርጋል፡፡ ይህን መሰረት በማድረግ የተከናወነው የአመለካከት መመዘኛ ውጤት እንዳመላከተው 3,362 (55.9%) የሚሆኑ መላሾች ነፃ የሆኑ ሲስተሞች፣ ሶፍትዌሮች፣ አፕሊኬሽኖችና ፀረ-ቫይረሶች መጠቀም በሳይበር ደህንነት ውስጥ ስጋት ወይም አደጋ ይሆናል ብለው እንደማያስቡ ያመላከቱ ሲሆን 2,655 (44.1%) የሚሆኑ መላሾች የሳይበር ስጋት እንደሚሆኑ አመላክተዋል፡፡

ምንም እንኳን 44.1 በመቶው ያህል መላሾች የሳይበር ደህንነት የሚፈልገውን አመለካከት ያላቸው ቢሆኑም ከፍተኛ ቁጥር ያላቸው የጥናቱ ተሳታፊዎች ውጤት እንደሚያሳየው ደግሞ ሰፊ የሆነ የአመለካከት ክፍተት እንደ ሀገር መኖሩንና የሳይበር ደህንነትን ለማስጠበቅ ከፍተኛ ስጋት እንደሚፈጥር መገንዘብ ይቻላል፡፡ ስለሆነም የአንድ ሰው ስህተት ወይም የአመለካከት ክፍተት በግለሰብ፣ በተቋም ብሎም በሀገር ደረጃ የተሳሰሩ ሲስተሞችንና ዲቫይሶችን ተጠቂ ሊያደርግ የሚችልበት ሁኔታ መኖሩ ክፍተቱን የጎላ ያደርገዋል፡፡

የሳይበር ደህንነት አመለካከት ትንተና የቀጠለ...



ግራፍ 3: የሳይበር ደህንነት አመለካከት ትንተና ውጤት

የማጥመድ ጥቃት አመለካከት- ከላይ እንደተገለፀው በሳይበር ደህንነት ውስጥ የሰው ልጅ ክፍተት ለሳይበር ጥቃት ምክንያት በመሆን ግንባር ቀደም ተጠቃሽ ነው፡፡ በመሆኑም የሰው ልጅ ደካማው የደህንነት ክፍተት ነው፡፡ ይህን የሰውን ልጅ ክፍተት የተረዱ የሳይበር ወንጀለኞች ማጥመድ ወይንም ፊሺንግ የተሰኘውን የጥቃት ዘዴ በመጠቀም ያለሙትን ኢላማ ያሳካሉ፡፡ ከማጥመድ ጥቃቶች መካከል ኢሜል ፊሺንግ ግንባር ቀደም ተጠቃሽ ነው፡፡ በመሆኑም ኢሜል ፊሺንግን መሰረት ያደረገ ጥቃትን ለመታደግ የተጠቃሚዎች የሳይበር ደህንነት አመለካከት በሚፈልገው ልክ መገራት ይኖርበታል፡፡

ይህን መሰረት በማድረግ የተጠናው ሃገራዊ ጥናት ውጤት እንደሚያመላክተው 3,814 (63.3%) የሚሆኑ መላሾች ስሙን ከማዉቀዉ ግለሰብም ሆነ ድርጅት የተላከልኝን ኢሜል አባሪ (Email attachment) ከፍቼ የመልዕክቱን ይዘት በማንበብ የምጎዳዉ ነገር አይኖርም የሚል ምላሽ ሰጥተዋል፡፡ በሌላ በኩል 2,212 (36.7%) የሚሆኑ መላሾች ጉዳት እንደሚደርስባቸው ያመላከቱ መሆናቸውን ውጤቱ ያሳያል፡፡

በመሆኑም ከፍተኛ ቁጥር ያላቸው የጥናቱ መላሾች ለኢሜል ማጥመድ ጥቃት ተጋላጭ የሚያደርግ ከፍተኛ የአመለካከት ችግር እንዳለባቸው ውጤቱ ያሳያል፡፡ ይህም እንደ ሀገር በተቋማትና ግለሰቦች ላይ ከፍተኛ ውድመት ሊያስከትል የሚችል የሳይበር ጥቃት ሰለባ የሚያደርግ ክፍተት ነው ብሎ መደምደም ያስችላል፡፡

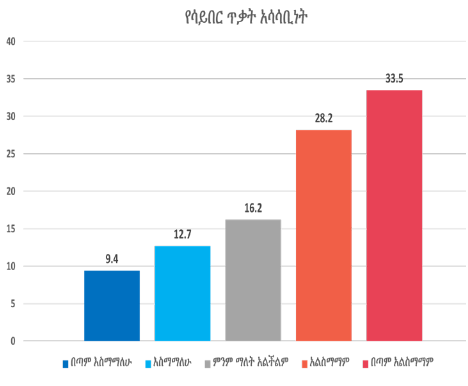
የማዘመኛ አመለካከት- በሳይበር ደህንነት ውስጥ የተለያዩ ሲስተሞችን እና መተግበሪያዎችን ወይንም አፕሊኬሽኖችን ማዘመን ከፍተኛ የደህንነት ጥሰትን የሚከላከል መፍትሔ ነው፡፡ ይህን መሰረት በማድረግ የተከናወነው የአመለካከት መመዘኛ ውጤት እንደሚያመላክተው 3,743 (62%) የሚሆኑ መላሾች የኮምፒውተርና ስልክ ሶፍትዌሮችን በየጊዜዉ ማዘመን (Updating) ከዉበት እና ቅልጥፍና ይልቅ የደህንነት ክፍተቶችን ለመድፈን ይረዳል የሚል ምላሽ ሰጥተዋል፡፡

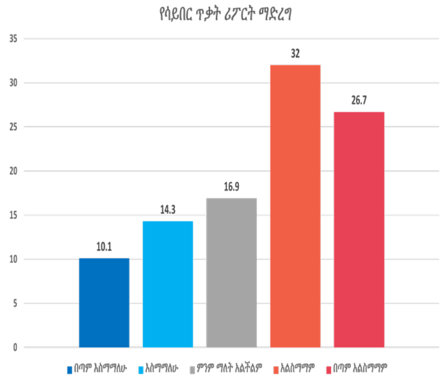
ይሁን እንጂ 2,290 (37.9%) የሚሆኑ መላሾች እንደማይስማሙ አመላክተዋል፡፡ በውጤቱ መሰረትም የማዘመን ጠቀሜታ በተመለከተ ከፍተኛ ቁጥር ያላቸው መላሾች መልካም አመለካከት እንዳላቸው መረዳት ቢቻልም 37.9 በመቶ የሚሆን የአመለካከት ክፍተት በሳይበር ደህንነት ላይ ሊደርስ ለሚችል ጥቃት በር በመክፈት ያለው ተፅእኖ ቀላል እንዳልሆነ የሚያሳይ የአመለካከት ክፍተት መሆኑን ውጤቱ አመላካች ነው፡፡

የተንቀሳቃሽ መረጃ ማከማቻዎች አመለካከት- የተንቀሳቃሽ መረጃ ማከማቻ ቁሶችን ስካን ማድረግ ከበርካታ ተንኮል አዘል ማልዌሮች መዛመት ይታደጋል፡፡ ይህን መሰረት በማድረግ የተከናወነው የአመለካከት መመዘኛ ውጤት እንደሚያመላክተው 3,379 (56.1%) የሚሆኑ መላሾች USB ፍላሽ ሁሌም ስካን ማድረግ ቶሎ እንዲበላሽ ስለሚያደርግ ሁሌም ከመጠቀሜ በፊት ስካን አላደርግም የሚል ምላሽ ሰጥተዋል፡፡

በሌላ በኩል 2,635 (43.8%) የሚሆኑ የጥናቱ ተሳታፊዎች ስካን ማድረግ ከብልሽት ጋር ግንኙነት እንደሌለው እና ከመጠቀማቸው በፊት ስካን እንደሚያደርጉ ምላሽ ሰጥተዋል፡፡ ይሁን እንጂ 56.1 በመቶ የሚሆን ከፍተኛ መጠንን የሚያመላክት የአመለካከት ክፍተት እንዳለ መገንዘብ፤ በሃገር አቀፍ ደረጃ ከሳይበር ደህንነት ባህሪ አንፃር ከፍተኛ ክፍተት መኖሩን ያመላክታል፡

የማህበራዊ ምህንድስና ጥቃት አመለካከት- የምንጠቀምባቸውን ኮምፒውተሮች ህዝብ በሚበዛበት ቦታ ክፍት አድርጎ መሄድ ለማህበራዊ ምንድስና ጥቃት ተጋላጭ ያደርጋል፡፡ ይህን አስመልክቶ የተደረገው ሀገራዊ ምዘና ውጤት 2,580 (42.7%) የሚሆኑ መላሾች የሚጠቀሙባቸውን ላፕቶፕ በስራ ቦታ፣በካፌ ውስጥም ብሎም ሰዎች በሚበዙባቸው ቦታዎች ለተወሰኑ ግዜያት ክፍት አድርገው መተው ምንም አይነት ጉዳት እንደማያጋጥማቸው በስምምነታቸው አረጋግጠዋል፡፡ 3,452 (57.2%) የሚሆኑ መላሾች በበኩላቸው እንዲህ ያለውን ድርጊት መፈፀም ጉዳት እንደሚያስከትልባቸው አረጋግጠዋል፡፡ በመሆኑም ከፍተኛ ቁጥር ያላቸው መላሾች ለሳይበር ደህንነት ማስጠበቅ ምቹ የሆነ አመለካከት እንዳላቸው ውጤቱ ያስረዳል፡፡





ግራፍ 4: የሳይበር ደህንነት አመለካከት መመዘኛ

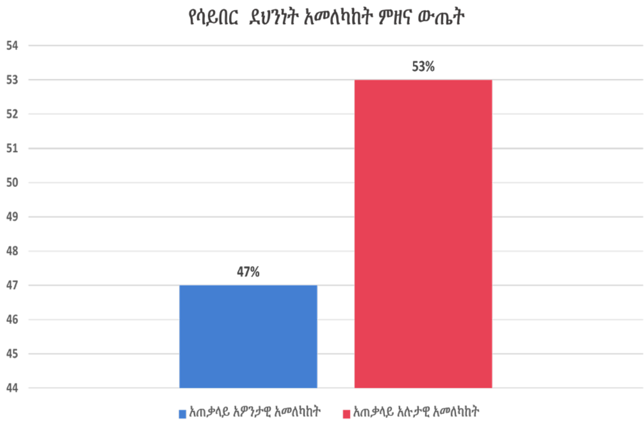
የሳይበር ጥቃት ኢላማ የመሆን አመለካከት- የሳይበር ደህንነት በ21ኛው ክፍለ-ዘመን የአለማችን ከፍተኛ ጉዳይ ከሆነ ሰነባብቷል፡፡ ሃገራችን ኢትዮጵያ በዚህ ምህዳር በሚደርሱ ጥቃቶች አንዷ ኢላማ ነች፡፡ ይህን መሰረት በማድረግ የተከናወነው የአመለካከት መመዘኛ ውጤት እንደሚያመላክተው 2,304 (38.3%) የሚሆኑ መላሾች የሳይበር ጥቃት ኢትዮጵያን ያን ያህል ሊያሳስባት የሚገባ አይደለም የሚል ምላሽ የሰጡ ሲሆን 3,711 (61.7%) የሚሆኑ መላሾች ጉዳዩ ኢትዮጵያንም የሚነዳና የሚያሳስባት መሆኑን በምላሻቸው አመላክተዋል፡፡

ይህም ከፍተኛ ቁጥር ያላቸው መላሾች መልካም አመለካከት እንዳላቸው መረዳት ቢቻልም 38.3 በመቶ የሚሆን የአመለካከት ክፍተት በቁልፍ መንግስታዊና ግላዊ ተቋማት ብሎም በማህበረሰብ ዘንድ ለሚሰነዘሩ ጥቃቶች አጋላጭ አመለካከቶች መኖራቸውን መረዳት ያስፈልጋል፡፡

የጥቃት ሪፖርት አመለካከት- በሀገራችን የግሉ ዘርፍ፣ በመንግስት ተቋማትና በማህበረሰብ ዘንድ የሳይበር ጥቃቶች እየደረሱ ይገኛል፡፡ ይሁን እንጂ የጥቃት ሪፖርትን ለሚመለከተው አካል የሚያቀርቡ በቁጥር ትንሽ ናቸው፡፡ ይህንም መሰረት በማድረግ በሀገር አቀፍ ደረጃ የተደረገው ጥናት የሚከተለውን ውጤት አመላክቷል፡፡

ከጠቅላላ መላሾች መካከል 2,495 (41.3%) የሚሆኑ መላሾች የሳይበር ጥቃት ደርሶ ሪፖርት ማድረጉ ችግሩን ስለማይፈታ ያን ያህል ጥቅም የለዉም ብለው የሚያምኑ ሲሆኑ 3,536 (58.7%) የሚሆኑ መላሾች ጥቅም አለው የሚለውን በመልሳቸው አረጋግጠዋል፡፡ በመሆኑም ከፍተኛ ቁጥር ያላቸው መላሾች የሳይበር ደህንነት የሚፈልገውን አመለካከት መላበሳቸውን ውጤቱ አመላክቷል፡፡

4.3.1 አጠቃላይ አማካኝ የአመለካከት ምዘና ውጤት



ግራፍ 5: አጠቃላይ አማካኝ የአመለካከት ምዘና ውጤት

በሳይበር ደህንነት ውስጥ ንቃተ-ህሊና ከፍተኛ ሚና አለው፡፡ በአለማችን ከ95 በመቶ በላይ የሳይበር ጥቃት የሚከሰተው የሰው ልጅ ለሳይበር ደህንነት ያለው ንቃተ-ህሊና አነስተኛ መሆን ጋር ይገናኛል፡፡ የሳይበር አጥቂዎች የሰውን ልጅ የእውቀት፣ የአመለካከትና የትግበራ ክፍተት በማነፍነፍ ከራሳቸው ኢላማ አንፃር ጥቃቶችን ይሰነዝራሉ፡፡ ይህን መሰረት በማድረግ በተደረገው ሀገር አቀፍ የሳይበር ደህንነት ንቃተ-ህሊና ጥናት አመለካከትን ለመለካት 18 የአመለካከት መለኪያዎች ተዘጋጅተው ለተጠኚዎች ቀርበዋል፡፡ ከ18 የአመለካከት መለኪያዎች መካከል 16 መለኪያዎች አሉታዊ (Negative) ይዘት ያላቸው ነበሩ፡፡ በመሆኑም 3,270 (54.2%) መላሾች ለቀረቡ አሉታዊ ይዘት ባላቸው መለኪያዎች ስምምነታቸውን የገለፁ ሲሆን 2,761 (45.8%) መላሾች በበኩላቸው የቀረቡት 16 መጠይቆች በሳይበር ደህንነት ላይ ከፍተኛ ጉዳት የሚያስከትሉ በመሆናቸው አለመስማማታቸውን አመላክተዋል፡፡

በሌላ በኩል 2,906 (48.3%) መላሾች ነፃ የህዝብ ዋይ-ፍይን በመጠቀም ሚስጢራዊ መረጃዎችን መለዋወጥ ለጥቃት (Hackers) ያጋልጣል ለሚለው አዎንታዊ ጥያቄ አዎ ያጋልጣል የሚል መልካም አመለካከት እንዳለቸው ውጤቱ ያመላከተ ሲሆን 3,103 (51.6%) መላሾች በበኩላቸው አያጋልጥም የሚል ምላሽን ሰጥተዋል፡፡ በተጨማሪም የሁለተኛውን አዎንታዊ መጠይቅ ትንታኔ ስናስቀምጥ ማለትም የአፕሊኬሽኖችንና ሌሎች የቴክኖሎጂ መተግበሪያዎችን ማዘመን ከውበትና ቅልጥፍና (Appearance) ይልቅ በዋናነት የሳይበር ደህንነት ክፍተቶችን ለመድፈን ይረዳል በሚል የተገለፀው የአመለካከት መመዘኛ ጥያቄ ላይ 3,743 (62%) የሚሆኑት መላሾች መስማማታቸውን የገለፁ ሲሆን በሌላ በኩል ደግሞ 2,290 (37.9%) የሆኑት መላሾች በጉዳዩ ላይ አለመስማማታቸውን ገልፀዋል፡፡ ይህም ማለት ምንም እንኳን አብዛኞቹ መላሾች 3,743 (62%) በጉዳዩ ላይ አዎንታዊ አመለካከት እንዳላቸው ቢታወቅም ወደ 37.9% የሚጠጋ የሳይበር ደህንነት አመለካከት ክፍተት መኖሩንም ያሳያል፡፡

በአጠቃላይ 3206 (53%) የሚሆኑት መላሾች ለሳይበር ደህንነት ያላቸው አመለካከት አሉታዊ ሲሆን 2823 (47%) መላሾች ደግሞ አዎንታዊ የሳይበር ደህንነት አመለካከት እንዳላቸው የጥናቱ ውጤት አመላክቷል፡፡ ስለሆነም በአዎንታዊ እና አሉታዊ የሳይበር ደህንነት አመለካከት መካከል የጥናቱ ውጤት ከፍተኛ ልዩነት እንዳለው በግልፅ ለመረዳት ያስችላል ፡፡ ይህም ከፍተኛ የሳይበር ደህንነት አመለካከት ችግር በሀገር አቀፍ ደረጃ በዋናነትም በኢትዮጵያ የኢንተርኔት ተጠቃሚ ዜጎች ላይ በስፋት እንደሚስተዋል የሚያመላክት ነው፡፡

4.4 የሳይበር ደህንነት ንቃተ-ህሊና አጠቃቀም/ልምምድ ትንተና (Practice analysis)

በዚህ ጥናት በኢትዮጵያ የኢንተርኔት ተጠቃሚ ዜጎች ላይ የሳይበር ደህንነት ንቃተ-ህሊና ሁኔታንና ደረጃን ለማወቅ ከተጠቀምንበት የ(KAP) ሞዴል ውስጥ የመጨረሻ ስልት የሆነውን የሳይበር ቴክኖሎጅ አጠቃቀም/ልምምድ ሁኔታን በሚመለከት በጥናቱ ከተገኙ መረጃዎች በመነሳት ትንተና በማካሄድ የተገኘውን ውጤት እንደሚከተለው ማስቀመጥ ተችሏል፡-

የሳይበር ደህንነት አጠቃቀምን (Practice) ለመለካት የተዘጋጀ መጠይቅ	አዎ	አይ
ለተለያዩ አካዉንቶቼ የይለፍ ቃል (Password) እንዳይረሳኝ አንድ አይነት ፓስወርድ እጠቀማለሁ	72.8%	27.2%
የሞባይል ስልኬ/ኮምፒዉተሬ በቫይረስ ያን ያህል ስለማይጠቃ ፀረ-ቫይረስ (Anti-vuris) አልጠቀምም	34.7%	65.2%
የተላከልኝን የኢሜል አባሪ(Email Attachment) ሁሉ ጠቃሚ እስከመሰለኝ ድረስ እከፍታለሁ	63.4%	36.6%
ለማህበራዊ ሚዲያ አካዉንቶቼ (Social Media Accounts) ወይም ለሌሎች አካዉንቶች ስም፣ ስልክ ቁጥር፣ የትዉልድ ዘመን እንደ ይለፍ ቃል (Pass-word) እጠቀማለሁ	51.3%	48.7%
ሞባይል ስልኬን/ኮምፒዉተሬን ማዘመን (Updating) አሰልችና ከፍተኛ ወጭ ስለሚጠይቅ በየግዜዉ አላዘምንም	55.5%	45.5%
የአንድሮይድ/አፕል አፕልኬሽኖችን (Android/Apple Applications) ከጎግል ፕሌይ ስቶር/አፕ ስቶር (Google Play Store/App Store) አውርጄ (Download) ተጠቅሜ አላዉቅም	57%	43%
ነጻ ዋይ ፍይ (Wi-Fi) ኢንተርኔት በመጠቀም ሚስጢራዊ ፋይሎችን/ዳታ እላላካለሁ	51.8%	48.2%
የምጠቀምበትን ስልክ/ኮምፒዉተር በስራ ቦታ፣ በካፌ ውስጥም ይሁን ሰዎች በሚበዙበት ቦታ ለተወሰኑ ግዜያት ክፍት ትቼ እሄዳለሁ	29.9%	70.1%
ትክክለኛ ድረ-ገጽን ለይቼ ስለማዉቅ ትክክለኛ ያልሆኑ ድረ-ገጾችን ከመጠቀም እቆጠባለሁ	64.4%	35.6%
የሳይበር ጥቃት/Hacking/ የደረሰብኝ መስሎ ከተሰማኝ ሪፖርት አደርጋለሁ	58.5%	41.5%
ፋላሽ ዲስክ (USB Flash) ወድቆ ካገኘሁ አንስቼ እጠቀማለሁ	54.6%	45.4%

ሰንጠረዥ 6: የሳይበር ደህንነት አጠቃቀም ትንተና

የሳይበር ደህንነት ንቃተ-ህሊናን ለመለካት ከሚረዱን ጉዳዮች ውስጥ አንዱ የሳይበር ደህንነት ባህሪ እና ባህልን ተግባራዊ ማድረግ ሲሆን የሳይበር ተጠቃሚ ዜጎች እውቀት እና አመለካከት ቢኖራቸውም እንኳ አተገባበራቸው ደካማ ከሆነ የሳይበር ደህንነት ንቃተ-ህሊና አላቸው ማለት አያስችልም፡፡
ከላይ በሰንጠረዡ በተገለፀው አጭር ትንተና መረዳት እንደሚቻለው የሳይበር ደህንነት አጠቃቀምን ለመለካት በወጡት ጥያቄዎች የዜጎችን የሳይበር ደህንነት ተግባር (Practice) በዝርዝር እንደሚከተለው ለማየት ያስችላል፡፡

የይለፍ ቃል- የሳይበር ደህንነትን ለማረጋገጥ የይለፍ ቃል አጠቃቀም ባህላችን ወሳኝ ሲሆን ለተለያዩ አካውንቶች ማለትም (ፌስቡክ፣ኢሜል፣ትዊተር እና ሌሎች የፋይናንስ ዝውውር የምናደርግባቸው አካውንቶች) ላለመርሳት በሚል ተመሳሳይ የይለፍ ቃል እጠቀማለሁ በሚል ከአጠቃላይ መላሾች መካከል 4399 (72.8%) የሚሆኑ ተጠቃሚዎች ለተለያዩ አካውንቶች ተመሳሳይ የሆኑ የይለፍ ቃሎችን እንደሚጠቀሙ መረዳት ተችሏል፡ ፡ ይህም ማለት የጥናቱ አብዛኛዎቹ የኢንተርኔት ተጠቃሚ ዜጎች የይለፍ ቃል አጠቃቀም በቀላሉ ለጥቃት ተጋላጭ እንደሆነ የሚያሳይ ነው፡፡

በሌላ ዕይታ የተሳታፊዎች ምላሽ እንደሚያመለክተው ለተለያዩ አካውንቶች የተለያዩ የይለፍ ቃሎችን የሚጠቀሙ ዜጎች 1641 (27.2%) ሲሆን ይህ የሚያሳየው ደህንነቱ የተጠበቀ የይለፍ ቃል አጠቃቀምን ከምናረጋግጥባቸው መንገዶች መካከል ለተለያዩ አካውንቶቻችን የምንጠቀመው የይለፍ ቃል የተለያየ እና ፍፁም ተቀራራቢነት የሌለው መሆን እንዳለበትና አዎንታዊ የሳይበር ደህንነት አጠቃቀም ትግበራ (Practice) መሆኑን ነው፤ ምክንያቱም ሳይበሩን የሚጠቀሙ ዜጎች የአንድ አካውንት ስርቆት ወይም ጥቃት ቢደርስበት ሌላውን አካውንት በተመሳሳይ የይለፍ ቃል ማግኘት ወይም ተደራሽ ማድረግ ስለሚያስችል ተመሳሳይ የይለፍ ቃል መጠቀም ለሳይበር ወንጀለኞች ምቹ ሁኔታን መፍጠር ስለሆነ ጥንቃቄ ማድረግ አስፈላጊ ነው፡፡

ጸረ-ቫይረስ አጠቃቀም- ኮምፒውተር ዲቫይስን እና ሌሎች ኤሌክትሮኒክ ዲቫይሶችን ስንጠቀም ፀረ-ቫይረስ መጠቀም አንዱ የሳይበር ጥቃት መከላከያ መንገድ ነው፡፡ ስለሆነም ስለፀረ-ቫይረስ ያላቸውን የአጠቃቀም ንቃተ-ህሊና ለመለካት በቀረበላቸው ጥያቄ መሰረት ከአጠቃላይ መላሾች መካከል 2093 (34.7%) የሚሆኑት የሞባይል ስልክ/ኮምፒዉተር በቫይረስ ያን ያህል ስለማይጠቃ ፀረ-ቫይረስ (Antivuris) አንጠቀምም የሚል ምላሽ የሰጡ ሲሆን ይህ ደግሞ የሚያሳየው ያልተጠበቀ የዲቫይስና የፀረ-ቫይረስ አጠቃቀም ክፍተት እንዳለ ያሳያል፡፡

ሌሎቹ 3932 (65.2%) የሚሆኑት መላሾች እንዳመላከቱት የሞባይል ስልክ/ኮምፒዉተር በቫይረስ ስለሚጠቃ ፀረ-ቫይረስ (Antivuris) እንጠቀማለን የሚሉ ናቸው፡፡ በመሆኑም ከውጤቱ መረዳት እንደሚቻለው ከግማሽ በላይ የሚሆኑት መላሾች ያላቸው የፀረ-ቫይረስ አጠቃቀም ባህል ጥሩ መሆኑን ያሳያል፡፡ በመሆኑም ኮምፒዩተራችንን እና ስልኮቻችንን ከሳይበር ጥቃት ለመከላከል ትክክለኛ ፀረ-ቫይረስ ከትክክለኛ ምንጭ አውርደን ወይም ህጋዊ እውቅና ካላቸው አካላት ገዝተን መጠቀም ተገቢ እና ሊበረታታ የሚገባ ባህሪ ነው፡፡

ደህንነቱ የተጠበቀ ኢ-ሜይል አጠቃቀም- ደህንነቱ የተጠበቀ የሳይበር ቴክኖሎጅ አጠቃቀም ከሚለካባቸው መንገዶች አንዱ የኢሜል መገናኛ ፕላትፎርም አጠቃቀም ነው፡፡ ይህንን ተግባራዊ ለማድረግ የዜጎችን ምላሽ ለማየት ስንሞክር ከአጠቃላይ የጥናቱ ተሳታፊዎች ውስጥ 3829 (63.4%) የሚሆኑት መላሾች የተላከላቸውን የኢሜል አባሪ (Email attachment) ሁሉ ጠቃሚ እስከመሰላቸው ድረስ ይከፍታሉ፡፡ ይህ የሚያሳየው ከግማሽ በላይ በሚሆኑ ዜጎች ላይ የኢሜል ደህንነት አጠባበቅና የአጠቃቀም ክፍተቶች እንደሚስተዋሉ ነው፡፡

ከጥያቄው ይዘት አውድ አንፃር እንደምክንያት ከሚጠቀሱት ጉዳዮች መካከል በዋናነት በኢሜል የሚላኩ ማናቸውም መልዕክቶች ሁሉ ጥሩ እና ትክክለኛ ይዘት አላቸው ተብሎ አይገመትም፡፡ በሌላ በኩል ደግሞ በኢሜል የሚላኩ መልዕክቶችና አባሪዎች ከትክክለኛ ምንጭ መሆን እና አለመሆናቸውን ማረጋገጥ አለመቻል ለምሳሌ፡- ተመሳሳይ ተቋም፣ ግለሰብ እና ድርጅትን በማስመሰል በሚላኩ የፊሽንግ ጥቃቶች ተጋላጭ እንዲሆኑ

ስለሚያደርግ የኢ-ሜይል አጠቃቀም ደህንነት ትኩረት ሊሰጠው የሚገባ የሳይበር ደህንነት ንቃተ-ህሊና መሻሻል ባህል ውስጥ አንዱ ወሳኝ ሃሳብ ነው፡፡

በዚሁ ሃሳብ ላይ 2207 (36.6%) የሚሆኑት ዜጎች የተላከላቸውን የኢሜል አባሪ ጠቃሚ ነው ብለው ቢያስቡም እንኳ በቀላሉ አይከፍቱም፡፡ ስለዚህ እነዚህ ዜጎች ደህንነቱ ስለተጠበቀ የኢሜል አጠቃቀም ሁኔታ አዎንታዊ ልምድ ያላቸው የኢንተርኔት ተጠቃሚ ዜጎች እንደሆኑ ለመረዳት ያስችላል፡፡ ይሁን እንጂ አብዛኛው ተሳታፊ በኢሜል የሚላኩ መልዕክቶችን ጠቃሚ ነው ብለው ካሰቡ እንደሚከፍቱ የመለሱ ሲሆን ይህም ጉዳይ ለሳይበር ጥቃት ኢጋላጭ የሚያደረግ የአጠቃቀም ልምድ በመሆኑ ተጠቃሚዎች የሚላኩላቸውን ኢሜሎች ከመክፈታቸው በፊት ምንጫቸውን ትክክለኛ መሆኑን ማረጋገጥ እንዲሁም አጠራጣሪ ሁኔታዎችን ከተመለከቱ መልዕክቶችንና ሊንኮችን እንዲሁም አታችመንቶችን ከመክፈት መቆጠብ ይኖርባቸዋል፡፡

ማህበራዊ ሚዲያ እና የሌሎች አካውንቶች አጠቃቀም- ዜጎች የሚጠቀሟቸውን የማህበራዊ ሚዲያ አካውንቶች ደህንነት ማስጠበቅ ሊደርስባቸው ከሚችል የሳይበር ጥቃት ለመከላከል ጉልህ ሚና እንዳለው ይታወቃል፡፡ የተለያዩ አካውንቶችን ደህንነት ለማስጠበቅ ከሚያግዙን ስልቶች መካከል በዋናነት ጠንካራ የይለፍ ቃል አጠቃቀም ወሳኝ ነው፡፡

ስለሆነም የማህበራዊ ሚዲያ እና ሌሎች አካውንቶችን ደህንነት ለማስጠበቅ የይለፍ ቃል አጠቃቀምን በሚመለከት በተጠየቁት ጥያቄ መሰረት ለማህበራዊ ሚዲያ አካዉንቶች (Social Media Accounts) ወይም ለሌሎች አካዉንቶች ስምን፣ስልክ ቁጥር፣ የትዉልድ ዘመንና የመሳሰሉትን እንደ ይለፍ ቃል (password) የሚጠቀሙት የጥናቱ ተሳታፊዎች ቁጥር 3100 (51.3%) ነው፡፡ ይህም ማለት ከግማሽ በላይ የሚሆኑት የኢንተርኔት ተጠቃሚ ዜጎች፤ የስልክ ቁጥርን፣ የትውልድ ዘመን እና መሰል ነገሮችን እንደ ይለፍ ቃል የሚጠቀሙ ናቸው ፡፡ በመሆኑም አብዛኛው ተጠቃሚ ቀላልና ደካማ የይለፍ ቃል በመጠቀም ለሳይበር ጥቃት ተጋላጭ እንደሆኑ የሚያመላክት ነው፡፡ ቀሪዎቹ 2943 (48.7%) የሚሆኑት ዜጎች ለማህበራዊ ሚዲያ እና ለሌሎች አካውንቶቻቸው ደካማ የይለፍ ቃል ማለትም የስልክ ቁጥር፣ የትውልድ ዘመን እና ስምን እንደ ይለፍ ቃል አይጠቀሙም፡፡

ስልክ/ኮምፒውተር ማዘመን- በሳይበር ቴክኖሎጅ ዘመን ዜጎች የሚጠቀሙበትን የሞባይል እና የኮምፒውተር ዲቫይስ ማዘመን የሳይበር ጥቃት ክፍተቶችን ለመዝጋት ያግዛል፡፡ ይህንን ታሳቢ በማድረግ ለተሳታፊዎች ሞባይል ስልክን/ኮምፒዉተርን ማዘመን (Updating) አሰልችና ከፍተኛ ወጭ ስለሚጠይቅ በየግዜዉ አናዘምንም ብለው ምላሽ የሰጡት የጥናቱ ተሳታፊዎች ቁጥር 3348 (55.5%) ሲሆኑ የሰጡት ምላሽ ከሳይበር ደህንነት መጠበቂያ መንገዶች ውስጥ ኮምፒውተርንና ስልክን እንዲሁም የተለያዩ መቃኛዎችን እና መተግበሪዎችን ማዘመን አሰልች እና ወጭ የሚያስወጣ በመሆኑ እንደማያዘምኑ አስቀምጠዋል፡፡

በሌላ መንገድ በንፅፅር ዝቅተኛ ቁጥር ያላቸው ዜጎች ማለትም 2683 (44.5%) የሚሆኑት መላሾች ደግሞ ስልካቸውን እና ኮምፒውተራቸውን እንደሚያዘምኑ መረዳት የተቻለ ቢሆንም ከግማሽ በላይ የሚሆኑት ዜጎች ማዘመን አሰልች እና ከፍተኛ ወጪ ያስወጣል በሚል አረዳድ እንደማያዘምኑ ከላይ በተገለፀው መንገድ መረዳት ተችሏል፡፡

ስለሆነም የኮምፒውተር፣የስልክ፣የመተግበሪያዎችና እና መቃኛዎችን (Browsers) ማዘመን ሊደርስ ከሚችለው የዜሮ ቀን (Zero day) ጥቃት ለመከላከል ከማገዙም ባሻገር ከተለያዩ አጥፊ ሶፍትዌሮች (ali-cious softwares) ይከላከላል፡፡

አፕልኬሽኖችን ከጎግል ፕሌይ ስቶር (Google Play Store)አዉርዶ የመጠቀም ልምድ- አብዛኛዉ የሳይበር ምህዳሩን የሚጠቀሙ የጥናቱ ተሳታፊዎች ማለትም 3441 (57%) ያህሉ ዜጎች የአንድሮይድ/አፕል አፕልኬሽኖችን (Android/Apple Applications) ከጎግል ፕሌይ ስቶር/አፕ ሰቶር (Google Play Store/App Store) አውርደዉ የሚጠቀሙ አይደሉም ወይም ከጎግል ላይ ነፃ መተግበሪያዎችን በማውረድ የሚጠቀሙ ናቸው።

በሌላ በኩል በጥናቱ ናሙና ከተወሰዱ 2597 ዜጎች ማለትም 43% የሚሆኑት መላሾች አፕልኬሽኖችን ከጎግል ፕሌይ ስቶር/አፕ ስቶር ወይም ከታማኝ ምንጮች አዉርደዉ የሚጠቀሙ ሲሆን ድርጊቱም አዎንታዊ የሳይበር ደህንነት አተገባበርን ያሳያል፡፡
ስለሆነም በኢትዮጵያ በተወሰነ ሁኔታም ቢሆን (43%) ያህሉ የሳይበር ምህዳር ተጠቃሚ ዜጋ የአፕሊኬሽኖችን አጠቃቀም በሚመለከት ታማኝነቱ ከሚታወቅ ምንጭ ወይም ከጎግል ፕሌይ ስቶር/አፕ ስቶር ላይ አፕሊኬሽን የማዉረድ ልምምድ እንዳለ የሚያስረዳ ሲሆን፤ ይህም በተጠቃሚዎች ላይ በቀላሉ ለሌሎች ተመሳሳይ፣ ፌክ እና ነጻ (Open) አጥፊ መተግበሪያዎች የመጋለጥ ሁኔታዎችን ይቀንሳል፤ ሆኖም ግን ቁጥሩ ቀላል የማይባል ዜጎች ወይም አብዛኞቹ የጥናቱ መላሾች አፕሊኬሽኖችን ከጎግል ፕሌይ ስቶር/አፕ ሰቶር ዉጭ የሆኑ ነጻ ወይም ከጎግል ፕሌይ ስቶር/አፕ ስቶር ጋር ተመሳሳይነት ያላቸዉ ፌክ አፕሊኬሽኖችን በማውረድ እንደሚጠቀሙ ጥናቱ ይጠቁማል፡፡ ይህም ሁኔታ ከፍተኛ ለሆነ የሳይበር ጥቃት ይዳርጋል ምክንያቱም አብዛኛዉን ጊዜ ነጻ እና ፌክ የሆኑ የመተግበሪያ ምንጮች የሚያቀርቧቸው አፕሊኬሽኖች በዋናነት የራሳቸዉን ድብቅ ዓላማ ለማሳካትና የተለያዩ መረጃዎችን ለመስረቅ ያግዛቸው ዘንድ ታሳቢ ተድርገው የሚለሙ የቴክኖሎጅ ውጤቶች ስለሚሆኑ መተግበሪያዎችን ከታማኝ ምንጭ አውርዶ መጠቀም ያስፈልጋል፡፡ ስለሆነም ደህንነቱ ያልተረጋገጠ አፕሊኬሽኖችን አዉርዶ መጠቀም በቀላሉ ለሶስተኛ ወገን የሳይበር ጥቃት አደጋ የሚያጋልጥ መሆኑ አጠያያቂ አይሆንም።

ነጻ ዋይ ፍይ (Wi-Fi) ኢንተርኔት የመጠቀም ልምምድ (Practice)- የጥናቱ መላሾች እንደገለጹት 3127 (51.8%) ነጻ ዋይ ፍይ (Wi-Fi) ኢንተርኔት በመጠቀም ሚስጢራዊ ፋይሎችን/ዳታ የሚላላኩ ሲሆን በሌላ በኩል 2910 (48.2%) የሚሆኑት መላሾች ደግሞ ነጻ ዋይ ፍይ (Wi-Fi) ኢንተርኔት በመጠቀም ሚስጢራዊ ፋይሎችን/ዳታ እንደማይላላኩ ጥናቱ ያሳያል።
በመሆኑም የኢንተርኔት ቴክኖሎጅ የሳይበር ምህዳር አንዱ አካል እንደመሆኑ መጠን ደህንነቱ በተጠበቀ መልኩ እና በአግባቡ መጠቀም ለሳይበር ደህንነት መጠበቅ ከፍተኛ አስተዋፅኦ አለው። ከዚህ ጋር በተገናኘ በ2019 በደቡብ አዉስትራሊያ ዩኒቨርሲቲ በተደረገ አንድ ጥናት «ነጻ ዋይ ፍይ (Wi-Fi) ኢንተርኔት መጠቀም እራስን የሳይበር ደህንነት አደጋ ዉስጥ እንደመክተት እንደሚቆጠር ይገለጻል / Using free public WiFi could put you at risk of a cyberattack /» ይላል።

ስለዚህ በኢትዮጵያ 51.8% የሚሆኑት የኢንተርኔት ተጠቃሚ ዜጎች ነጻ ዋይ ፍይ (Wi-Fi) ኢንተርኔት በመጠቀም ሚስጢራዊ ፋይሎችን/ዳታ የመላላክ ልምድ ያላቸዉ በመሆናቸዉ ድርጊታቸው ለከፍተኛ የሳይበር ጥቃት የሚያጋልጥ እንደሆነ ይህ ጥናት ያስረዳል።

የሚጠቀሙበትን ኮምፒዉተር ዲቫይስ ክፍት አድርጎ የመሄድ ልምምድ/Practice/- አብዛኛዉ ዜጎች ማለትም 4215 (70.1%) የሚጠቀሙበትን ስልክ ወይም ኮምፒዉተር ዲቫይስ በስራ ቦታ፣ በካፌ ውስጥም ይሁን ሰዎች በሚበዙበት ቦታ ለተወሰኑ ግዜያት ክፍት ትቶ የመሄድ ልምድ እንደሌለ ጥናቱ ይጠቁማል፤ ሆኖም ግን 1796 (29.9%) የሚሆኑት የሳይበር ምህዳሩን የሚጠቀሙ ዜጎች የሚጠቀሙበትን ስልክ ወይም ኮምፒዉተር በስራ ቦታ፣በካፌ ውስጥም ይሁን ሰዎች በሚበዙበት ቦታ ለተወሰኑ ግዜያት ክፍት ትቶ የመሄድ መጥፎ ልምምድ እንደሚያደርጉም ጭምር ከጥናቱ መረዳት ይቻላል፡፡ ይህ መጥፎ ልምምድ /Practice/ቁጥሩ ይነስ እንጂ የግለሰብ እና የተቋማት ሚስጥራዊ መረጃዎች መሰረቅ ወይም መሰል ተግባራት መከሰት እንደምክንያት ስለሚያገለግል ለሳይበር ጥቃት መፈፀም እንደ ወሳኝ መንገድ ተደርጎም ይቆጠራል፡፡

ከዚህ ጋር በተያያዘ ትንተና ኮምፒውተርን፣ ስማርት ስልኮችን ወይም ታብሌቶችን በሕዝባዊ ቦታዎች ላይ ግላዊ መረጃዎችን መከፈትና መጠቀም ብቻ ሳይሆን የኮምፒዉተር ዲቫይሶችን ክፍት አድርጎ የመሄድ መጥፎ ልምምድ እንዳለ ዓለም አቀፍ የሳይበር ደህንነት ጥናቶች ያሳያሉ፡፡

ትክክለኛ ድረ-ገጽን ለይቶ የመክፈት ልምምድ/Practice/- የትክክለኛ ድረገጽ አጠቃቀም ልምምድን በተመለከተ ትክክለኛ ድረ-ገጽን ለይተዉ በማወቅ ትክክለኛ ያልሆኑ ድረ-ገጾችን ከመጠቀም የሚቆጠቡት የጥናቱ ተሳታፊዎች 3890 (64.7%) ሲሆኑ፤ በሌላ በኩል ትክክለኝ እና ትክክለኛ ያልሆኑትን ድረ-ገፆች ሳይለዩ የሚከፍቱ የኢንተርኔት ተጠቃሚ ዜጎች ቁጥር ደግሞ 2141 (35.6%) ናቸዉ፡፡

ስለሆነም ምንም እንኳ ጥናቱን መሰረት በማድረግ በአብዛኛው ትክክለኛ ድረ-ገፆችን ለይቶ የመጠቀም የተሻለ ልምምድ ቢኖርም ትክክለኛ ድረ-ገጽን ለይቶ አለመጠቀም የባለቤትነት ምስክርነቶችን/Credentials/ ፣ የባንክ ሂሳብ መረጃዎችን፣ የኢሜል ልዉዉጦችን እና መሰል መረጃዎችን ሚስጥራዊነት ለመሰረቅ፣ መቀየር ወይም ተደራሽ እንዳይሆን ስለሚያደርግ ከፍተኛ የሆነ የቴክኖሎጅ አጠቃቀም ጥንቃቄን ይፈልጋል፡፡ ብዙ የሳይበር ደህንነት ጥናቶች እንደሚያሳዩት ሃሰተኛ ድረ-ገጽ የመጠቀም ልምምድ ለኢሚል መረጃ ስርቆት እና ለባንክ አካውንት ስርቆት መፈፀም የአንበሳዉን ድርሻ እንደሚወስድ ያስረዳሉ፡፡

የሳይበር ጥቃት/Hacking/ ሪፖርት የማድረግ ልምምድ/Practice/- በተቋም ወይም በግለሰብ ደረጃ የሳይበር ጥቃትን ሪፖርት የማድረግ ጉዳይን በተመለከተ 3533 (58.5%) የሳይበር ምህዳር ተጠቃሚ ዜጎች የሳይበር ጥቃት ሲያጋጥማቸዉ ሪፖርት የሚያደርጉ ሲሆን 2507 (41.5%) ያህሉ የሳይበር ምህዳር ተጠቃሚ ዜጎች የሳይበር ጥቃቱን ሪፖርት እንደማያደርጉ በጥናቱ ተመላክቷል፡፡

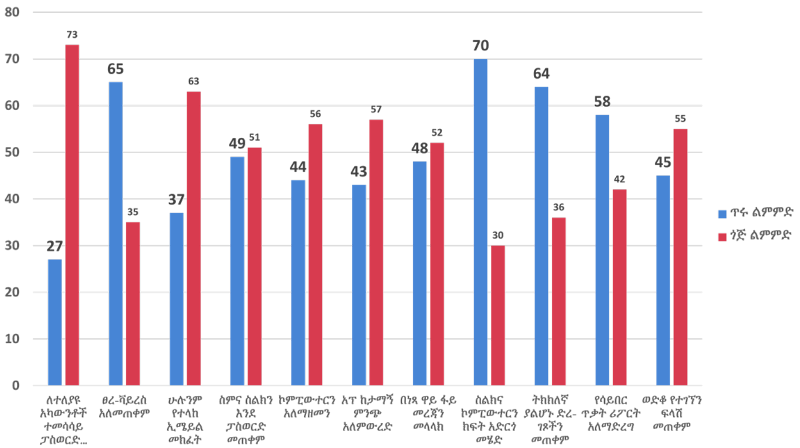
በመሆኑም የሳይበር ጥቃት በማንኛውም ጊዜና ቦታ የሚከሰት ክስተት ስለሆነ እንዲሁም የሳይበር ጥቃት ከጊዜ ወደ ጊዜ ዉስብስብነቱና የጥቃቱ ደረጃ እየጨመረ የሚሄድ ጉዳይ በመሆኑ የሳይበር ጥቃት ናቸዉ ተብለዉ የሚታሰቡ ክስተቶችንና አጠራጣሪ ሁኔቶች ሁሉ መመዝገብና ለሚመለከተው አካል ሪፖርት መደረግ እንዳለባቸዉ የሳይበር ደህንነት ተቋማት ከማሳየታቸውም በተጨማሪ በሳይበር ቴክኖሎጅ ዘመን እንደ ሳይበር ደህንነት ንቀተ-ህሊና ባህል ተደርጎ ከሚታሰቡ ሃሳቦች መካከል አንዱ ነው፡፡

ወድቆ የተገኘ ፍላሽን አንስቶ የመጠቀም ልምምድ/Practice/- በጥናቱ የተካተቱት የሳይበር ምህዳር ተጠቃሚ ዜጎች ምላሽ እንደሚያመለክተዉ 3297 (54.6%) የሚሆኑት የጥናቱ ተሳታፊዎች ፋላሽ ዲስክ

(USB Flash) ወድቆ ካገኙ አንስተዉ እንደሚጠቀሙ የገለፁ ሲሆኑ 2740 (45.4%) የሚሆኑት ደግሞ ፋላሽ ዲስክ (USB Flash) ወድቀዉ ካገኙ የማይጠቀሙ ናቸዉ።፡

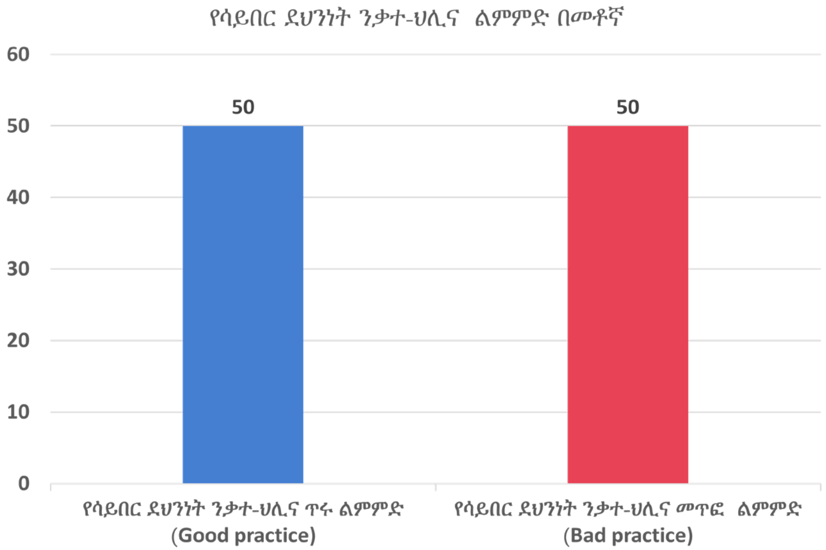
በጥናቱ ውጤት መሰረት ቁጥሩ ቀላል የማይባል የሳይበር ምህዳር ተጠቃሚ ዜጎች ወድቆ የተገኘን ፍላሽ ዲስክ መጠቀም በከፍተኛ ሁኔታ ለሳይበር ጥቃት የሚያጋልጥ መጥፎ ልምምድ/Bad practice/ እንዳላቸው ጥናቱ ያሳያል። ከዚህ ጋር በተያያዘ ፍላሽ ዲስክ እና ተንቀሳቃሽ የመረጃ ማከማቻ መሳሪያዎች (Removable devices) ለማልዌር ጥቃት እና መሰል የሳይበር ጥቃት ምንጭ ከሆኑ መሳሪያዎች መካከል ዋነኞቹ ናቸዉ። ስለሆነም ወድቆ የተገኘን ፍላሽ መጠቀም በተለይ ለማልሽየስ ኮድ ወይም ጥቃት /Malicious code attack/ እና ለማህበራዊ ምህንድስና /Social engineering/ የጥቃት አይነቶች እንደሚያጋልጥ ሬድ ቲም ሰኪዩሪቲ (Red Team security 2016) የተባለ ድርጅት ይገልጻል። በ2016 በተካሄደ ጥናት ለጥናቱ ሲባል ከወደቁ 297 ፋላሽ ዲስኮች ውስጥ (USB Flash) 98% የሚሆኑት እንደተነሱና በተጨማሪም በጥቂት ቀናት ዉስጥ 45% የሚሆኑት ወደ ኮምፒዉተር ዲቫይሶች እንደተሰኩና ሰፋፊ የሳይበር ጥቃት ሙከራዎች ማድረግ እንደሚቻል በጥናት አረጋግጠዋል።

በመሆኑም ወድቆ የተገኘን ፍላሽ ወይም ማንኛውንም ተንቀሳቃሽ የመረጃ ማከማቻ ዲቫይሶች አንስቶ መጠቀም በራስ ፍቃድ ለሳይበር ጥቃት መጋለጥ ከመሆኑም በላይ ለከፍተኛ መረጃ ምዝበራ እና መሰል የሳይበር ጥቃት ሁነቶች የሚያጋልጥ መሆኑን ሬድ ቲም ሰኪዩሪቲ (Red Team Security) የተባለው ድርጅት ያስረዳል።



ግራፍ 6: የሳይበር ደህንነት ጥሩ ልምምድ እና መጥፎ ልምምድ

4.4.1 አጠቃላይ አማካይ የሳይበር ደህንነት አጠቃቀም/ልምምድ ምዘና ውጤት



ግራፍ 7: የአጠቃላይ አማካኝ የሳይበር ደህንነት አጠቃቀም/ልምምድ ውጤት

የሳይበር ደህንነት ንቃተ ህሊና ለመገንባት እና ወደ ባህል እንዲሸጋገር ለማድረግ የሳይበር ደህንነት እዉቀት ማዳበር (Knowledge)፣ እዉቀትን በጥሩ አመለካከት መቃኘት (Attitude) እና ወደ ጥሩ ልምምድ (Practice) ሽግግር ማድረግ እንደሚገባ የተለያዩ የሳይበር ደህንነት ሞዴሎች ያስረዳሉ።

በጥናቱ መሰረት በአማካኝ (Mean) 50% የሳይበር ደህንነት እሳቤዎችንና እዉቀቶችን በጥሩ ልምምድ (Good practice for cyber security awareness) በማስደገፍ የሚተገበር እንደሆነ መረዳት ይቻላል። በሌላ እይታ ደግሞ 50% ያህሉ አጠቃላይ መላሾች የሳይበር ደህንነት ንቃተ-ህሊና ሁኔታ በጥሩ ልምምድ ያልተደገፈ ወይም ጎጅ የሆነ የሳይበር ደህንነት አጠቃቀም እንዳለ ያሳያል።

ስለሆነም የሀገርን፣የተቋማትን፣የግለሰብን በአጠቃላይ የዜጎችን የሳይበር ቴክኖሎጅ የአጠቃቀም ደህንነት ለማስጠበቅ ከ 3 ምሰሶዎች (Pillars) ውስጥ በልምምድ ላይ የተመሰረተ የሳይበር ደህንነት ንቃተ ህሊና አንዱ መሆኑ የሚያጠያይቅ ጉዳይ ባለመሆኑና ቁጥሩ ቀላል የማይባል ማለትም 50% ያህሉ የጥናቱ ውጤት ለሳይበር ደህንነት አጋላጭ የሆነ ጎጅ ልምምድ እንዳለ በግልፅ ያስረዳል፤ ይህም እንደ ሀገር ወደፊት ሰፋፊ የንቃተ-ህሊና ስራዎች መስራት እንደሚገባቸው ያመላክታል፡፡

4.5 አጠቃላይ የሳይበር ደህንነት ንቃተ-ህሊና ሁኔታ በኢትዮጵያ (Cyber security awareness)

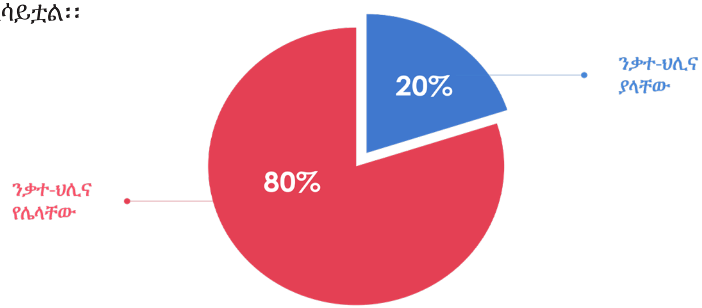
ይህ ጥናት መሰረታዊ በሆነ መንገድ የሳይበር ደህንነት ንቃተ-ህሊና ደረጃን ለመለካት የሳይበር ደህንነት እውቀት፣ አመለካከት እና የአተገባበር ሁኔታን መሰረት በማድረግ ተካሂዷል፡፡ ይህም አተያይ በዋናነት በብዙ የሳይበር ደህንነት ንቃተ-ህሊና ፕሮግራሞችና ጥናቶች ላይ ጥቅም ላይ የሚውለውን ሞዴል (KAP-model) በመጠቀም በኢትዮጵያ የኢንተርኔት/የሳይበር ተጠቃሚ ዜጎች ላይ ያለውን የሳይበር ደህንነት ንቃተ-ህሊና ደረጃ ለማወቅ ያስችላል፡፡

በዚህ መሰረት ከላይ የጥናቱን ዝርዝር ዓላማዎች ከግምት ውስጥ በማስገባት የተደረገውን የትንተና ውጤት በመጠቀምና ወደ አንድ ጥቅል ሃሳብ በመሰብሰብ (Conceptual mapping) አጠቃላይ የሆነ የሳይበር ደህንነት ንቃተ-ህሊና ደረጃን ለማወቅ ይቻላል፡፡

አጠቃላይ የሳይበር ደህንነት የእውቀት ደረጃን በሚመለከት በአራት ክፍሎች አማካኝነት የተተነተነ ሲሆን፤ ምንም እውቀት የሌላቸው (No knowledge) 1742 (29.23%)፣ ዝቅተኛ እውቀት (Low knowledge) 2126 (35.62%)፣ መካከለኛ እውቀት (Medium) 701 (11.75%) እና ከፍተኛ እውቀት (High knowledge) 1396 (23.4 %) በሚል ተተንትኗል፡፡

በዚህ መሰረት በአጠቃላይ የእውቀት ደረጃ ልኬት እይታ እውቀት የሌላቸውና ዝቅተኛ የእውቀት ደረጃን ከግምት ውስጥ በማስገባት ማለትም 3868 (64.85 %) የሚሆነው ዉጤት የሳይበር ደህንነት እውቀት የሌላቸው እንዲሁም 2097 (35.15%) የሚሆነው ደግሞ የሳይበር ደህንነት እውቀት ያላቸው መሆኑን ያሳያል፡፡
የጥናቱን የሳይበር ደህንነት የአመለካከት ውጤት በሚመለከት ጠቅለል ተደረጎ ከላይ እንደተገለፀው 2823 (47%) ያህሉ የጥናቱ ተሳታፊዎች አዎንታዊና 3206 (53%) ያህሉ አሉታዊ አመለካከት አላቸው በሚል አጠቃላይ መላሾች ለሳይበር ደህንነት ያላቸውን የአመለካከት ውጤት ተመላክቷል፡፡

በመጨረሻም አጠቃላይ የጥናቱን የሳይበር ደህንነት የአተገባበር ውጤት በሚመለከት 3024 (50.2%) የሚሆኑት የጥናቱ መላሾች አዎንታዊ የሳይበር ደህንነት የአተገባበር ውጤት እንዲሁም 3007 (49.8%) የሚሆኑት ደግሞ አሉታዊ የሳይበር ደህንነት አተገባበር ውጤት በኢትዮጵያ የኢንተርኔት ተጠቃሚ ዜጎች ላይ እንደሚስተዋል ጥናቱ አሳይቷል፡፡



ግራፍ 8: አጠቃላይ የሳይበር ደህንነት ንቃተ-ህሊና ደረጃ በኢትዮጵያ

በመሆኑም ከላይ በግራፉ እንደተመላከተው በኢትዮጵያ የኢንተርኔት ተጠቃሚ ዜጎች አጠቃላይ የሳይበር ደህንነት ንቃተ-ህሊና ደረጃን (የእውቀት፣ አመለካከትና አተገባበርን) ለመለካት ክሩገር እና ሌሎች (2006) ያነሱትን ሀሳብ ከግምት ወስጥ ማስገባት ያስፈልጋል፡፡ ይህም በጥናቱ ጽንሰ-ሀሳባዊ ፍሬምወርክ ላይ እንደተመላከተው የሳይበር ደህንነት ንቃተ-ህሊናን በ KAP ሞዴል ተጠቅመን በምናጠናበት ወቅት ንቃተ-ህሊና አላቸው የሚባለው የእውቀት፣ አመለካከትና ትግበራ የጋራ ወጤትን (hared/intersectional value) በመውሰድ እንደሆነ ተገልጧል፡፡ በዚህ መሰረት በኢትዮጵያ የኢንተርኔት/ሳይበር ተጠቃሚ ዜጎች ላይ 20% ያህል የሳይበር ደህንነት ንቃተ-ህሊና ያላቸው እንዲሁም (80%) ያህል ደግሞ የሳይበር ደህንነት ንቃተ-ህሊና የሌላቸው መሆኑን ጥናቱ በግልፅ ያሳያል፡፡

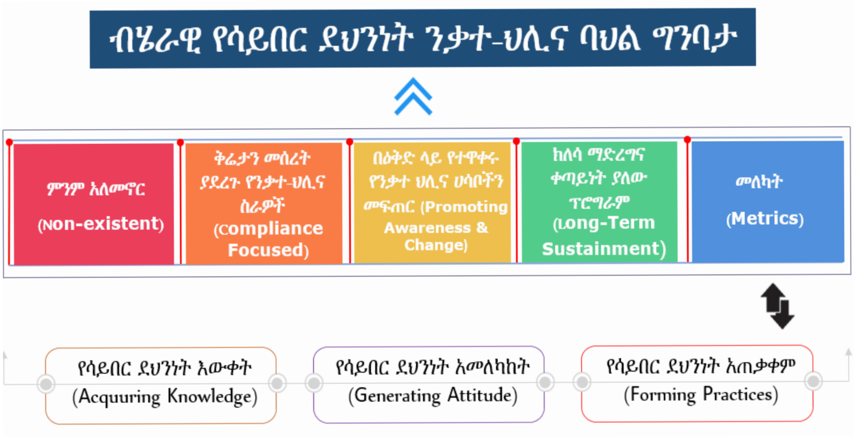
በሌላ በኩል በጥናቱ የስነ-ህዝብ መረጃዎች ትንተና መሰረት የጥናቱ ተሳታፊዎች የትምህርት ደረጃን በሚመለከት በጥቅሉ 77.3% ያህሉ ዲፕሎማ፣ዲግሪና ማስተርስ እንዲሁም ፒ ኤች ዲ እንዳላቸው ተመላክቷል፤ እንዲሁም 87.5 % ያህሉ ተሳታፊዎች ደግሞ ከ14-35 የእድሜ ክልል ውስጥ እንደሚገኙ የተመላከተ ሲሆን፤ ከጥናቱ አጠቃላይ ውጤት አንፃር ስንመለከተው ደግሞ በኢትዮጵያ የሳ/ደ/ን/ ህሊና ጉዳዮችን በሚመለከት ተለምዷዊ የሆነውን የስነ-ትምህርት ስርዓት በማሳደግና በማስፋፋት ብቻ ችግሩን መቅረፍ እንደማይቻል እና በሀገራችን ይህ ከፍተኛ የሆነ የሳይበር ደህንነት ንቃተ-ህሊና ክፍተት ለሁሉም የቴክኖሎጂ ተጠቃሚ ዜጋ እኩል ስጋት እንደሆነ ያመላክታል፡፡

4.6 የጥናቱ ትንተና አጭር ማጠቃለያ

የዚህ ጥናት ዋና ዓላማ በውጤት ደረጃ ከላይ በዝርዝርና በአማካይ የጥናት ምዘና ውጤት ሂደት ውስጥ በግልፅ ተቀምጧል፡፡ በመሆኑም በኢትዮጵያ የኢንተርኔት ተጠቃሚ ዜጎች ውስጥ ያለው አጠቃላይ የሳይበር ደህንነት ንቃተ-ህሊና ደረጃ ልኬታ (Measurement) መሰረቱን የሚያደርገው በ (SANS) የሳይበር ደህንነት ንቃተ-ህሊና እና ባህል ግንባታ የእድገት ሞዴል (Maturity model) አማካኝነት እንደሆነ መረዳት ይቻላል፡፡

ስለሆነም በሳይበር ደህንነት ንቃተ-ህሊና የእድገት ሞዴል ውስጥ በተካተቱት አምስቱ (5) የንቃተ-ህሊና እድገት ደረጃዎችና ንቃተ-ህሊና የመፍጠሪያ ስልቶች ውስጥ ማለትም የሳይበር ደህንነት ንቃተ-ህሊና ምንም አለመኖር (non-existent)፣ ቅሬታን መሰረት ያደረጉ የንቃተ-ህሊና ስራዎች (Compliance focused) ፣ በእቅድ ላይ የተዋቀሩ የንቃተ-ህሊና ሀሳቦችን መፍጠር (Promoting awareness and change)፣ ከለሳ ማድረግና ቀጣይነት ያለው ፕሮግራም (Longterm sustainement) እንዲሁም መለካት (Metrics) በመባል የተገለፁትን ሃሳቦች ከግምት ውስጥ በማስገባት ይህ ጥናት በሀገራችን ያለውን የሳይበር ደህንነት ንቃተ-ህሊና ደረጃ መለካትን አንግቦ ሲነሳ በዋናነት ሁሉንም ደረጃዎች ለመዳሰስ ሞክሯል፡፡

ይህም የጥናቱን ንድፈ-ሃሳብ (KAP model or conceptual framework of the study) እንደ መለኪያ (Metrics) በመጠቀም የሀገራችንን የኢንተርኔት ተጠቃሚ ዜጎች የሳይበር ደህንነት ንቃተ-ህሊና ደረጃ ለማወቅ ያስችላል ማለትም 20 በመቶው የሆነ የሳይበር ደህንነት ንቃተ-ህሊና ደረጃ በሀገር አቀፍ ደረጃ እንደሚስተዋል አመላክቷል፡፡ በሌላ በኩል ደግሞ በሳይበር ተጠቃሚዎች ውስጥ በግለሰብ ደረጃ፣ በተቋማት እንዲሁም በሀገር ደረጃ ያለውን ዝቅተኛ የሳይበር ደህንነት ንቃተ-ህሊና ደረጃ ለማሻሻል ብሎም ባህል ለመገንባት (SANS's maturity model) ይህ ንድፈ-ሃሳብ (KAP model) ይጠቅማል፡፡ ይህ አጭር አጠቃላይ የትንተና ሃሳብ በሚከተለው ስዕላዊ መግለጫ ተመላክቷል፡፡



ምስል 4፡ የጥናቱ ትንተና ማጠቃለያ

ምዕራፍ አምስት

ማጠቃለያና ምክረ-ሃሳብ

5.1 ማጠቃለያ (Conclusion)

ይህ ጥናት በሀገር አቀፍ ደረጃ ያለውን የኢንተርኔት/የሳይበር ተጠቃሚ ዜጎች የሳይበር ደህንነት ንቃተ-ህሊና ደረጃን ማወቅ ዋና ዓላማው በማድረግ የጥናቱን ውጤት በሶስት ዋና ዋና የዕይታ መስኮች ለመለካት ተሞክሯል፡፡

የመጀመሪያው ሀሳብ በኢትዮጵያ የሳይበር ተጠቃሚ ዜጎችን የእውቀት ደረጃ መለካት የነበረ ሲሆን ይህንኑ ዓላማ ለመመለስ በጥናቱ መጠይቅ ውስጥ በተካተቱት ጥያቄዎች መሰረት አጠቃላይ በኢትዮጵያ የኢንተርኔት ተጠቃሚዎች ውስጥ 65 በመቶው በጣም ዝቅተኛ የእውቀት ደረጃ እንዲሁም ቀሪው 35 በመቶው ብቻ ከፍተኛ ሊባል የሚችል የሳይበር ደህንነት ንቃተ-ህሊና እውቀት እንዳለ ከጥናቱ የተገኘው ውጤት አመላክቷል፡ ፡ ከነዚህ የእውቀት ደረጃን ለመለካት ጥናቱ ከተጠቀማቸው ጥያቄዎች ውስጥ ተጠቃሚዎች ራሳቸውን ከኮምፒዉተር/ሞባይል ቫይረስ ጥቃት ራስን ለመከላከል ማድረግ ስለሌሉብን ጉዳዮች፣ ስለ ጸረ-ቫይረስ ትክክል ያልሆኑ ሀሳቦች እንዲሁም የኢሜል (Email) አካዉንት እንዴት ሊሰረቅ (Hack) ሊደረጉ እንደሚቻል በሚሉ ዝርዝር መለኪያዎች በጣም አነስተኛ የሆነ የእውቀት ደረጃ እንደተሰተዋለ ጥናቱ ያመለከተ ሲሆን የነዚህ ሃሳቦች አማካይ ዝቅተኛ የእውቀት ደረጃም 78.1 በመቶው ነው፡፡

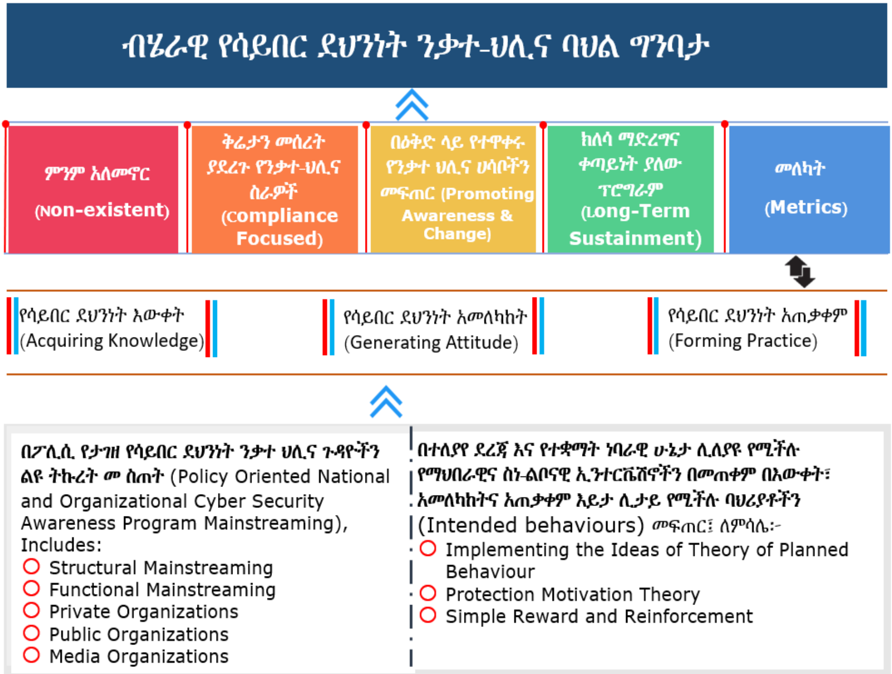
ሌላኛው የመተንተኛ መንገድ ደግሞ የሳይበር ደህንነት አመለካከት ሲሆን፤ በዚህ የመመዘኛ ስልት መሰረት የተካሄደው የጥናት ውጤትም 53 በመቶው አሉታዊ/ዝቅተኛ የሳይበር ደህንነት አመለካከት እንዲሁም 47 በመቶው አዎንታዊ የሳይበር ደህንነት አመለካከት በኢትዮጵያ የኢንተርኔት/የሳይበር ተጠቃሚ ዜጎች ላይ እንደሚስተዋል ጥናቱ አሳይቷል፡፡

በመጨረሻም የጥናቱ የሳይበር ቴክኖሎጅ ተጠቃሚዎች በኢትዮጵያ 49.8 በመቶው ጥሩ/አዎንታዊ የሳይበር ቴክኖሎጅ አጠቃቀም ልምምድ እንዳላቸው እንዲሁም ቀሪው 50.2 በመቶው ደግሞ ጎጅ/አሉታዊ የሳይበር ደህንነት ልምምድ በሀገር አቀፍ ደረጃ እንዳለ ለማወቅ ተችሏል፡፡

በአጠቃላይ ይህ ጥናት በኢትዮጵያ የኢንተርኔት/የሳይበር ተጠቃሚ ዜጎችን የሳይበር ደህንነት ንቃተ-ህሊና ደረጃ ለማወቅ ዋና ዓላማው አድርጎ የተከናወነ ሲሆን ውጤቱም 20 በመቶ አዎንታዊ የሳይበር ደህንነት ንቃተ-ህሊና በሀገር አቀፍ ደረጃ እንዳለ ጥናቱ ያስረዳል፡፡ ይህ የጥናት ውጤት የሚያመላክተው ከሳይበር ምህዳሩ ባህሪ እና በአግባቡ መጠቀም ካልተቻለ ሊያስከተለው ከሚችለው ውድመት አንፃር እጅግ ከፍተኛ የሆነ ትኩረትን የሚሻ ጉዳይ መሆኑንና ጉዳቱን መቀነስ የሁሉም የቴክኖሎጅው ተጠቃሚዎች ሃላፊነት እንደሆነ መረዳት መቻልን ነው፡፡

5.2 ምክረ-ሃሳብ (Recommendations)

በምክረ-ሀሳብ ደረጃ ይህ ጥናት ምንም እንኳን የጥናቱ ውጤት በንፅፅር እጅግ በጣም ዝቅተኛ የሆነ የሳይበር ደህንነት ንቃተ-ህሊና የእውቀት ደረጃ ከአመለካከትና የአጠቃቀም ደረጃ አንፃር እንዳለ ከማሳየቱም በተጨማሪ በሶስቱም መለኪያዎች አማካይ የጥናት ውጤት ሲታይም በሀገር አቀፍ ደረጃ በጣም ዝቅተኛ የሚባል የሳይበር ደህንነት ንቃተ-ህሊና እንዳለ ለማረጋገጥ ተችሏል፡፡ ስለሆነም ይህን ሁኔታ ለማሻሻል በሀገር አቀፍ ደረጃ ሊተገበሩ የሚገቡ ጉዳዮችን በሚከተለው መልኩ ለማስቀመጥ ተችሏል፡-



ምስል 5፡ የጥናቱ ምክረ-ሀሳብ

ይህ ከላይ በምስሉ የተመላከተው አጭር ምክረ-ሃሳብ በዋናነት የሚያጠነጥነው በሁለት ወሳኝ ጉዳዮች ላይ ሲሆን፤ የመጀመሪያው ሃሳብ የሳይበር ደህንነት ንቃተ-ህሊና ፕሮግራም ሜንስትሪሚንግን መርህ ማድረግ ነው፡፡ ይህ የሜንስትሪሚንግ ስርዓትም የሚጀምረው በሀገር አቀፍ ደረጃ ህግና ፖሊሲዎችን በማርቀቅ በግልም ይሁን በመንግስት ተቋማት ውስጥ ተፈፃሚነት የሚኖራቸው የአወቃቀር (Structural mainstreaming) እንዲሁም ለሚዘረጉት የሳይበር ደህንነት የአወቃቀር ስርዓቶች አስፈላጊውን ባለሙያና አመራር እንዲሟላ በማስቻል ተጨባጭ ተግባር ውስጥ መግባት መቻል (Functional mainstreaming) ያስፈልጋል፡፡ ስለሆነም ይህ የሳይበር ደህንነት ንቃተ-ህሊና ሜንስትሪሚንግ ሃሳብ በተለይ የሚዲያ ተቋማት አስቸኳይ ትኩረት ሰጥተው ቢሰሩበት የሃሳቡን ቅቡልነትና የአፈፃፀም እንዲሁም ሀገራችን አሁን ካለችበት እጅግ ዝቅተኛ የሳይበር ደህንነት ንቃተ-ህሊና ደረጃና ሊያስከትለው ከሚችለው የሳይበር ጥቃት ለመዳን የራሱ የሆነ ጉልህ ሚና ይኖረዋል፡፡

በሁለተኛ ደረጃ የተመላከተው ምክረ-ሃሳብ ደግሞ ትኩረቱን የሚያደርገው የሳይበር ደህንነት ንቃተ-ህሊና ፕሮግራም ሜንስትሪሚንግ ከተካሄደ በኋላ እንደተቋማት እና የሳይበር ቴክኖሎጅው ተጠቃሚዎች ነባራዊ ሁኔታ ሊለያዩ የሚችሉ ዝርዝር የንቃተ-ህሊና ሃሳቦችንና በሳይበር ደህንነት ንቃተ-ህሊና አስፈፃሚ ክፍል (Department) ውስጥ ተቀባይነት የሚኖራቸውን የሳይበር ደህንነት የእውቀት፣ አመለካከትና ትግበራ ሂደቶችን ለመፍጠር የሚያግዙ ፅንሰ-ሃሳቦችንና ንድፈ-ሃሳቦችን መፍጠር እንዲሁም መተግበር ያስፈልጋል፤ ለምሳሌ፡-የፐላንድ ቢሄብየርና ፕሮቴክሽን ሞቲቬሽን ቲዮሪ (The ideas of theory of planned behavior and protection motivation theory) በተጨማሪም የማበረታቻና ተመጣጣኝ ቅጣት (Reward and punishment) ስርዓቶችን መከተል የሚል ጥቅል ምክረ-ሃሳብ ቀርቧል፡፡

ማጣቀሻ ጽሁፎች (References)

Abeselom Negussie .2015. Practices, Challenges And Prospects Of Informaiton Secuirty Policy In Ethiopian Banking Industry

Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes, 50(2), 179-211.

Bandura, A., & Walters, R. H. 1977. Social learning theory (Vol. 1): Englewood cliffs Prentice Hall.

Borodzicz, E. 2005. Risk, crisis and security management. Chichester: John Wiley & Sons.

Central Statistical Services of Ethiopia .2007. Population and Housing Census report.

Cohen, L. M., & Manion, L. 2000. L. and Morrison. Research methods in education, 5.

Creswell, J. W., Plano Clark, V. L., Gutmann, M. L., & Hanson, W. E. 2003. Advanced mixed methods research designs. Handbook of mixed methods in social and behavioral research, 209(240), 209-240.

DATAREPORTAL .2022. DIGITAL 2022: ETHIOPIA, Reports

Ethio telechom .2018/19. Yearly report, retrieved, https://www.ethiotelecom.et/2018-19-efy-p-report/

Frankel, J. R., & Wallen, N. E. 2007. How To Design and Evaluate Reseach in Education. Edisi 6. In: New York: The Mc Graw Hill Companies

GSMA Intelligence Data Report .2019. The mobile gender gap report 2019. GSMA, London.

IBM. 2014. IBM Security services 2014 cyber security intelligence index. Analysis of cyber attack and incident data from IBM's worldwide security services operations

IBM. 2015. Cyber security intelligence index. Analysis of cyber attack and incident data from IBM's worldwide security services operations.

INSA .2022. Ethio-CERT's yearly report

International Organization for Standardization & International Electrotechnical Commission .2016. ISO 27000: 2016. Information technology-security techniquesInformation security management systems-Overview and vocabulary. ISO.

International Telecommunications Union. 2008. ITU-TX.1205: series X: data networks, open system communications and security: telecommunication security: overview of cyber security.

International Telecommunications Union. 2011. ITU national cyber security strategy guide.

Jang-Jaccard, J., & Nepal, S. 2014. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973-993.

Jung, P. W. 2011. A critical analysis on the concept of "cyber cecurity". Yonsei Journal of Medical and Science Technology Law, 2(2), 1-25.

Krejcie, R.V. & Morgan, D.W. 1970. Determining sample size for research activities. Educational and Psychological Measurement, 30, 607-610.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness, Computers & Security, 25(4), 289-296

Orr, G. 2003. Diffusion of innovations, by Everett Rogers (1995). Retrieved January, 21, 2005.

OTA (2018/2019). Cyber Incident Breach Trends Report

Royal Society .1992. Risk analysis, perception, management. London: Royal Society.

Safa, N. S., Von Solms, R., & Furnell, S. 2016. Information security policy compliance model in organizations. Computers & Security, 56, 70–82.

Serianu (2018):"Africa Cyber Security Report".

Sjöberg, Lennart. 2000. "Risk Perception by the Public and by Experts: A Dilemma in Risk Management." Human Ecology Review, vol. 6, no. 2, pp. 1–9. JSTOR,

Steven, J. (2012). Cybersecurity and National Security: Global Perspectives. Academic Press.

Symantec.2017.Internetsecuritythreatreport.Retrievedfrom https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Von Solms, R., & Van Niekerk, J. 2013. From information security to cyber security. Computers & Security, 38, 97-102.

Vorwelget, V., & Haubringer, F. (2015). The impact of social media on political discourse. Journal of Communication Studies, 28(3), 120-135.

Warkentin, M., & Willison, R. 2009. Behavioral and policy issues in information systems security: The insider threat. European Journal of Information Systems, 18(2), 101.

Willis, J. W., Jost, M., & Nilakanta, R. 2007. Foundations of qualitative research: Interpretive and critical approaches. London: Sage.

Woretaw, A., & Lessa, L. 2012. Information Security Culture in The Banking Sector in Ethiopia. 5th ICT 2012 Ethiopia Conference, (p. 22 pages). Addis Ababa.

World population review .2019. Central Statistical Agency of Ethiopia (provided by Clive Thornton).

Yamane, Taro .1967. Statistics, An Introductory Analysis, 2nd Ed., New York: Harper and Row